319-CD-004-003

EOSDIS Core System Project

CSMS Integration and Test Plan for the ECS Project Volume 2: Release A

Final

June 1995

Hughes Information Technology Corporation
Landover, Maryland

CSMS Integration and Test Plan for the ECS Project Volume 2: Release A

June 1995

Prepared Under Contract NAS5-60000
CDRL Item 054

SUBMITTED BY

Ed Lerner /s/ 6/30/95

Ed Lerner, CSMS Segment Manager Date
EOSDIS Core System Project

Hughes Information Technology Corporation
Landover, Maryland

319-CD-004-003

This page intentionally left blank.

Preface

This document is a formal contract deliverable with an approval code 1. It requires Government review and approval prior to acceptance and use. Documents with approval code 1 are formal contract deliverables which require Government review and approval prior to acceptance and use. This document is under ECS Contractor configuration control. Once this document is approved, Contractor approved changes are handled in accordance with Class I and Class II change control requirements described in the EOS Configuration Management Plan. Changes to this document shall be made by document change notice (DCN) or by complete revision.

Any questions should be addressed to:

Data Management Office
The ECS Project Office
Hughes Information Technology Corporation
1616 McCormick Drive
Landover, MD 20785

This page intentionally left blank.

Abstract

This document specifies the Test Plan (Release A) for the Communications and Systems Management Segment (CSMS) of the ECS Project. It includes descriptions of: the CSMS test methodology, Build/Thread functional decomposition, detailed test cases, requirements traceability matrices between Level 4 requirements and test cases, and descritpions of resources and test tools needed for these tests. The information provided in this plan will serve as a baseline for developing the follow up test procedures (DID 322).

Keywords: integration, test, I&T, build, thread, Release-A, CSMS, MSS, CSS, ISS, ECS, DCE, Traceability, level 4, test case(s), requirements, test tools

This page intentionally left blank.

Change Information Page

List of Effective Pages	
Page Number	**Issue**
Title	Final
iii through xiv	Final
1-1 and 1-2	Final
2-1 and 2-2	Final
3-1 through 3-12	Final
4-1 through 4-92	Final
5-1 through 5-18	Final
A-1 and A-2	Final
B-1 through B-100	Final
C-1 through C-4	Final
AB-1 through AB-5	Final

Document History			
Document Number	**Status/Issue**	**Publication Date**	**CCR Number**
319-CD-004-001	Review Copy	December 1994	
319-CD-004-002	Final	March 1995	
319-CD-004-003	Final	June 1995	

This page intentionally left blank.

Contents

4. CSMS Release A Test Descriptions

5. CSMS Hardware/Performance Test Descriptions

1. Introduction

1.1 Identification

This document is submitted as required by CDRL item 054, DID 319/DV1 whose requirements are specified as a required deliverable under the Earth Observing System (EOS) Data and Information System (EOSDIS) Core System (ECS), Contract (NAS5-60000).

1.2 Scope

This document defines the plan for integration, test, and verification of the Communications and System Management Segment, referred to as CSMS, for each Release. There is a separate document for each proceeding release. It is one of three segment test plans required to test ECS at the segment level. There is a separate test plan for the Flight Operations Segment (FOS) and the Systems and Data Processing Segment (SDPS). The CSMS Integration and Test Plan applies only to segment and element level verification activities. This plan includes verifying that the ECS complies with the CSMS Level 4 Functional Requirements, and the ECS design specifications. The roles and activities of the Communications and System Management Segment Integration and Test Organization (CSMS I&T) are described and schedules for performing CSMS I&T activities are included.

This document reflects the Technical Baseline submitted via contract correspondence no. ECS 194-00343.

1.3 Purpose

This Segment/Element Integration and Test Plan describes the test, review, and analysis effort to be conducted by the CSMS I&T organization for the Release A CSMS Segment/Elements. This document presents the overall processes and activities associated with verifying the CSMS Segment/Element during the segment integration and test phase of the CSMS development. This test plan provides an outline of the activities to be performed for CSMS I&T, and is later used to prepare test procedures which provide more detailed instructions for verification of the CSMS software. It delineates the roles and responsibilities of each organization associated with the segment integration and test activities.

1.4 Status and Schedule

The EOSDIS Core System, Contract Data Requirements Document specifies the Segment/Element Integration and Test Plan (DID 319/DV1) is delivered two weeks prior to each PDR and IDR. In order to support the development of CSMS software in releases this plan is updated on an incremental delivery schedule dependent on major releases and reviews such as PDR and IDR.

As a PDR document, this document discusses the CSMS I&T process which includes a Build Thread Plan for CSMS I&T of its elements and subsystems for Release A. The Build and Thread Tests are described at a summary level identifying test objectives, inputs, outputs, and success

criteria. Test databases and test tools needed for each test are identified. Corresponding documents including tests for Release B, C, and D will be provided at appropriate IDRs.

This submittal of DID 319/DV1 meets the milestone specified in the Contract Data Requirements List (CDRL) of NASA contract NAS5-60000. It is anticipated that this submittal will be reviewed during the appropriate segment- or system-level Preliminary Design Review (PDR), and that subsequent changes to the document will be incorporated into a resubmittal according to a schedule mutually agreed to by GSFC and ECS.

1.5 Organization

This document, which is based on Release A requirements, is organized into five chapters:

Section 1 Introduction, contains the identification, scope, purpose and objectives, status and schedule, and document organization.

Section 2 Related Documents, provides a bibliography of parent, applicable and reference documents for the CSMS Segment Integration and Test Document.

Section 3 CSMS Segment Integration and Test Overview, describes the process used to integrate and test the CSMS Segment and subsystems.

Section 4 CSMS Segment Test Descriptions, describes the specific segment level thread and build tests, which will be used to verify the functionality of the CSMS Segment.

Section 5 CSMS Hardware/Performance Test Descriptions, describes the tests which will be used to verify the functionality of the CSMS hardware and some of the performance resource issues.

Appendix A Contains a list and brief description of the test tools needed for CSMS Segment Integration and Test (Release A).

Appendix B Contains the requirements traceability matrix, mapping test cases to Level 4 requirements (Release A).

Appendix C Contains the CSC to Build/Thread Description Matrix (Release A).

Abbreviations and Acronyms Contains a listing of abbreviations and acronyms used in this Document.

2. Related Documents

2.1 Parent Documents

The parent documents are the documents from which this CSMS Integration and Test Plan's (Release A) scope and content are derived.

101-101-MG1-001	Project Management Plan for the EOSDIS Core System
194-107-MG1-XXX	Level 1 Master Schedule for the ECS Project
194-201-SE1-001	Systems Engineering Plan for the ECS Project
301-CD-002-003	System Implementation Plan for the ECS Project
402-CD-001-002	System Integration and Test Plan for the ECS Project, Volume 1: Interim Release 1 (IR-1), Final
402-CD-002-002	System Integration and Test Plan for the ECS Project, Volume 2: Release A, Final
194-501-PA1-001	Performance Assurance Implementation Plan for the ECS Project
423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work
423-41-02	Goddard Space Flight Center, Functional and Performance Requirements Specification (F&PRS) for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS)
423-41-03	Goddard Space Flight Center, EOSDIS Core System (ECS) Contract Data Requirements Document

2.2 Applicable Documents

The following documents are referenced within this CSMS Integration and Test Plan (Release A), or are directly applicable, or contain policies or other directive matters that are binding upon the content of this volume. The following documents are available on the ECS Data Handling System (EDHS); http://edhs1.gsfc.nasa.gov/Info/pdr/440wp01info.html

194-207-SE1-001	System Design Specification for the ECS Project
319-CD-003-002	CSMS Integration & Test Plan (IR-1)
194-401-VE1-002	Verification Plan for the ECS Project, Final
409-CD-001-003	ECS Overall System Acceptance Test Plan for Release A, Final
194-415-VE1-002	Acceptance Testing Management Plan for the ECS Project, Final

2.3 Information Documents

2.3.1 Information Documents Referenced

The following documents are referenced herein and, amplify or clarify the information presented in this document. These documents are not binding on the content of the ECS CSMS Integration and Test Plan (Release A).

194-102-MG1-001	Configuration Management Plan for the ECS Project
193-103-MG3-001	Configuration Management Procedures for the ECS Project
305-CD-003-002	CSMS Design Specifications for the ECS Project

2.3.2 Information Documents Not Referenced

The following documents, although not referenced herein and/or not directly applicable, do amplify or clarify the information presented in this document. These documents are not binding on the content of the CSMS Integration and Test Plan (Release A).

104-CD-001-003	Data Management Plan for the ECS Project
193-105-MG3-001	Data Management Procedures for the ECS Project
194-219-SE1-018	Interface Requirements Document Between EOSDIS Core System (ECS) and Tropical Rainfall Measuring Mission (TRMM) Ground System

3. CSMS Integration and Test Overview

This section contains an overview of the approach taken by the Communications and Systems Management Segment Integration and Test organization to ensure complete and thorough testing at the segment level. Included is information concerning the CSMS I&T environment, schedules and verification activities and responsibilities.

3.1 CSMS I&T and the ECS Environment

3.1.1 CSMS Functional Overview

ECS is comprised of three segments, each comprised of various subsystems. The three segments are the Flight Operations Segment (FOS), Science Data Processing Segment (SDPS) and Communications and Systems Management Segment (CSMS). Each of these segments are decomposed into subsystems and the subsystems are composed of CIs. This document will test the design and implementation of the CSMS CIs and their integration into ECS subsystems.

CSMS is responsible for the interconnection of users and service providers, the transfer of information between ECS components and systems management. CSMS is also responsible for supporting and providing interoperability for the Science Data Processing Segment (SDPS) and the Flight Operations Segment (FOS). CSMS contains three internal subsystems: Communications Subsystem (CSS), Inter networking Subsystem (ISS) and the Systems Management Subsystem (MSS). CSS is a collection of services that are responsible for providing flexible interoperability and information transfer between clients and servers. ISS is a layered stack of communications services corresponding to layers 1-4 of the OSI-RM. MSS is made up of a collection of applications that are responsible for the management of all ECS resources, including all SDPS, FOS, ISS and CSS components.

The CIs for CSMS at Release A are listed in Table 3.1-1. Included are CI names and CSMS subsystems. A short description of each CI is given following Table 3.1-1.

Table 3.1-1. CSMS Release A CIs

CI	Subsystem Superclass
Management Software CI (MCI)	MSS
Management Logistics CI (MLCI)	MSS
Management Agent CI (MACI)	MSS
Management Hardware CI (MHCI)	MSS
Distributed Computing Software CI (DCCI)	CSS
Distributed Communications Hardware CI (DCHCI)	CSS
Internetworking CI (INCI)	ISS
Internetworking Hardware CI (INHCI)	ISS

Management Software CI (MCI). The Management Software CI includes both Enterprise System Monitor and Local System Manager Configurations.

Management Logistics CI (MLCI). The Management Logistics CI includes both the managing of the Enterprise Logistics Manager and Domain Logistics Manager Configurations.

Management Agent CI (MACI). The Management Agent CI includes the agent specializations. An agent is the interface to a managed object. An agent system is a device, which has the responsibility of performing network management operations requested by the manager.

Management Hardware CI (MHCI). The Management Hardware CI includes: local management of ECS sites enterprise-wide (ECS-wide) monitoring and coordination, shared workstation and server pool for enterprise and domain managers, as well as enterprise-wide (ECS-wide) monitoring and coordination.

Distributed Computing Software CI (DCCI). The Distributed Computing Software CI includes the client and server configurations. This CI includes the DCE COTS package, which is the baseline distributed computing technology chosen through Release B.

Distributed Communications Hardware CI (DCHCI). The Distributed Communications Hardware CI includes the communications servers, such as; E-mail server, directory server, security server, time server, trader server and bulletin board (user registration/toolkit distribution) server.

Internetworking CI (INCI). The Internetworking CI includes the COTS implementations of the communication protocols reserved by network nodes. This includes protocols and standards for layer four and below of the OSI/ISO reference model (e.g., TCP, IP, OSPF, RIP).

Internetworking Hardware CI (INHCI). The Internetworking Hardware CI includes all COTS network devices and cabling: routers, hubs, switches, and test equipment. It does not include host interface cards.

3.1.2 CSMS I&T Organization Relationship to Other Test Groups

The CSMS I&T organization is responsible for integration and test at the subsystem level. This includes acceptance of software components upon completion of unit testing, integration of these components into segment subsystems, complete and thorough testing of the integrated software, and recording and reporting of any problems encountered during testing. Integrated software units are tested against Level 4 requirements documented in the Segment/Element Requirements Specification (ECS document number 304-CD-003-001). The CSMS I&T organization is responsible for verifying functional components and intra segment interfaces. When necessary the interfaces will be simulated.

The CSMS I&T group interacts with and supports other ECS and independent test organizations. This includes the Quality Office, Systems Integration and Test, the Independent Acceptance Test Organization (IATO), and EOSDIS Independent Verification and Validation (IV&V) Contractor. The IATO monitors segment tests and identifies any Level 3 requirements that can be verified through analysis of segment test results. The IV&V contractor monitors ECS verification activities.

The Quality Office assists in identifying training needs of test personnel and schedules formal training. The Quality Office conducts requirements traceability audits during the Implementation

and Integration and Test phases as each test case is completed and evaluated. They are responsible for monitoring the hardware inspection and unit-level verification procedures and verifying segment and system test plans for completeness. They also validate segment and system integration and tests and test results. The Quality Office participates in segment test implementation, reviews, and analysis. They are also responsible for monitoring the life cycle of the nonconformance reports and participating in the final decision on product acceptability.

Upon completion of CSMS testing, the software is delivered to the ECS System I&T organization. This group is responsible for integration and test of the CSMS and SDPS deliverables at the system level. Starting with Release A, System I&T is also responsible for FOS integration as well. This includes verification of all SDPS and CSMS segment software. The System I&T organization starts with the highest level builds at the segment level and uses them as system threads for tests. These threads are then combined into system level builds and tested. The system builds may include system threads derived from different segments. These builds are aggregated with other system threads (previously tested) and/or other tested builds, which are also tested. This process is repeated for all of the system builds until the entire release is integrated and tested. Testing is done to confirm compliance to Level 3 requirements documented in the Functional and Performance Requirements Specification (Goddard document number 423-41-02) and the System Design Specification (ECS document number 194-207-SE1-001). Internal interfaces are tested with ECS software and hardware where available. Informal verification of the external interfaces is accomplished during the Systems I&T phase using simulators or locally devised tests to reduce the risk of acceptance testing with immature external interfaces.

The Independent Acceptance Test Organization (IATO) is provided with the system level builds upon completion of testing by the Systems I&T Organization. Acceptance testing involves preparation at the EDF prior to CSR (Consent to Ship Review), and formal testing at the operational centers after CSR. Testing at the operational centers provides the IATO an opportunity to test using the unique operational configuration of each operational center. By testing on site and emphasizing science and operational scenarios, acceptance testing will be functioning in more of a "real-world" environment than the previous levels of testing. Most Level 3 requirements will be verified through formal release acceptance testing at ECS centers. However, to alleviate some of the work that is involved in release acceptance testing at the ECS centers, some level 3 requirements will be verified at the acceptance level by analyzing the results of the segment and systems I&T at the EDF. This will only occur for requirements that can be satisfied by inspecting the results of the segment and system I&T test results.

Upon completion of the RRR (Release Readiness Review), the Independent Verification and Validation (IV&V) contractor provides an independent assessment of the functionality and performance of ECS releases. The IV&V contractor is responsible for pre-operational testing performed at the ECS centers and the validation of the ECS Level 3 requirements. They are also responsible for the reporting and tracking of non conformance identified during this phase of testing. The IATO, which serves as the ECS contractor's primary contact for the IV&V contractor, supports the IV&V test team at the ECS centers. The IV&V contractor has access to all ECS contractor test activities and technical information. The IATO coordinates the resources required for testing by the IV&V contractor at each of the ECS centers.

3.2 CSMS I&T Organization Testing Approach

The CSMS I&T organization will integrate and verify CSMS CI functionality on an incremental basis. As incremental integration and testing proceeds, larger portions of the segment are assembled.

3.2.1 Segment I&T Functional Testing

As unit testing on software and hardware items is completed, the CSMS I&T organization incrementally assembles lower-level functionality into progressively higher levels until a segment is completely integrated and tested. Functional components that are integrated are threads, and the result of combining threads is a build. Functional testing verifies Level 4 functional requirements.

3.2.2 CSMS Build/Thread Methodology

The build/thread concept, which is based on the incremental aggregation of functions, is used to plan CSMS I&T activities. A CSMS thread is the set of components (software CIs, hardware and data) and operational procedures that implement a function or set of related functions at the segment level. Threads are tested individually to facilitate Level 4 requirements verification and to isolate software problems. A build is an assemblage of threads to produce a gradual buildup of segment capabilities. This orderly progression of combining lower level software and/or hardware items to form higher level items with broader capability is the basis of CSMS integration. The build tests are generally regression tests of the threads and/or builds that make up the build. CSMS builds are combined with other CSMS builds and threads to produce higher level builds. Verification of threads and builds is accomplished at progressively higher levels as the CSMS software is assembled for each release.

CSMS build/thread diagrams are developed for each release. The build/thread diagram for Release A is presented in Figure 3.2-1. Threads and builds are defined by examining CSMS CIs, Level 4 requirements and segment/element design specifications. The CSMS I&T organization with support from the CSMS development community, logically groups the CSMS release into functional categories divided along noticeable boundaries. These categories are the basis for CSMS threads. Threads are combined to define CSMS builds. Builds include several integrated thread functions. The build/thread diagram for each CSMS release acts as a framework for definition of CSMS test case definition. From each build and thread on the diagram, test cases are developed. These test cases provide the basis for development of step-by-step test instruction to be documented as CSMS test procedures.

The CSMS build/thread diagrams and other ECS segment level diagrams (FOS and SDPS), are combined to create a foundation for the build/thread diagrams developed for System level testing (ECS System Integration & Test Plan). CSMS and other segment build/thread testing provides an approach for first-level testing and validation of component functionality at the segment level. System I&T combines segment level build/threads into a system release which validates ECS design against Level 3 requirements and user needs.

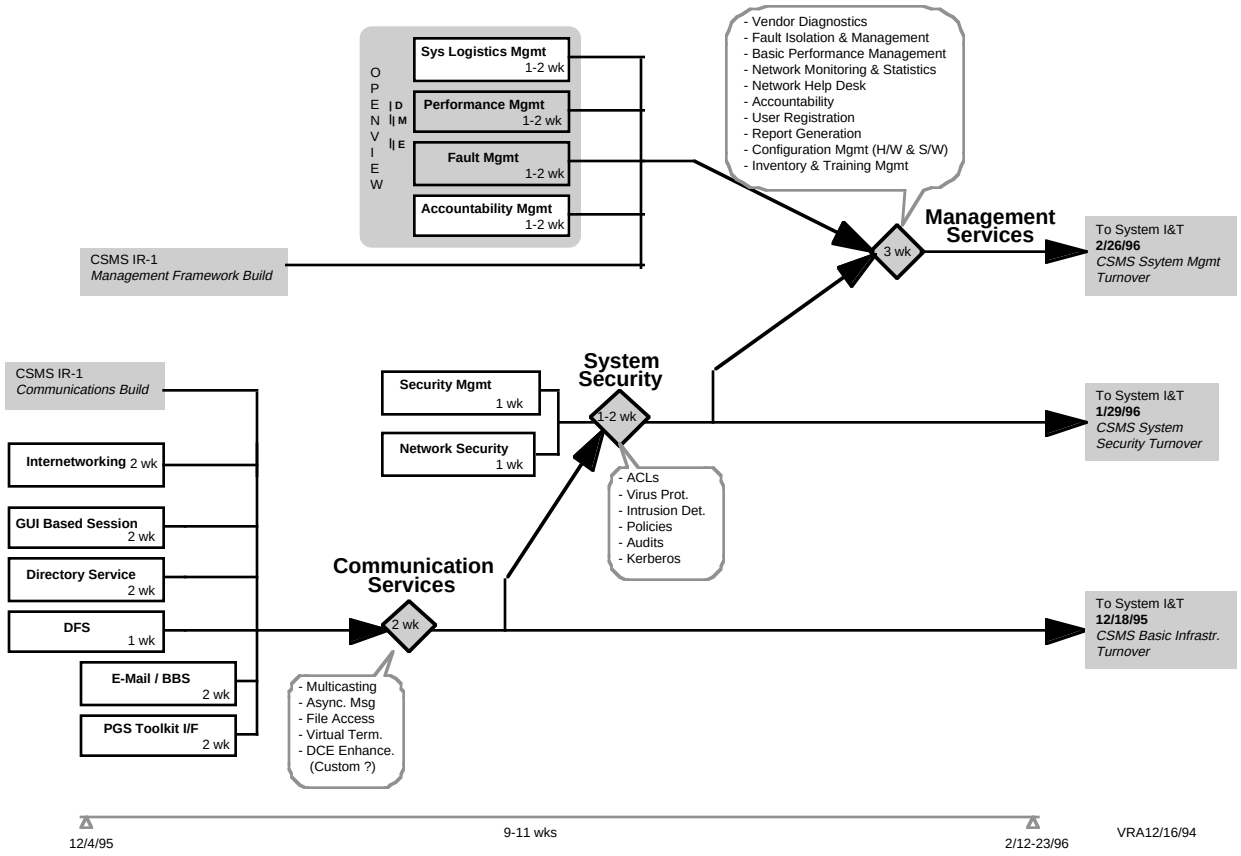

Figure 3.2-1. Release A CSMS Build/Thread Diagram

3.3 CSMS I&T Test Verification

The following sections define responsibilities and activities of the CSMS I&T organization. CSMS I&T verification includes definition of verification methods, post test analysis, regression testing, and verification resources.

3.3.1 Verification Methods

The four verification methods used for CSMS I&T include: inspection, analysis, demonstration, and test. As defined in the ECS Verification Plan (ECS document number 194-401-VE1-002).

a. Inspection. The visual, manual examination of the verification item and comparison to the applicable requirement or other compliance documentation, such as engineering drawings.

b. Analysis. Technical or mathematical evaluation based on calculation, interpolation, or other analytical methods.

c. Demonstration. Observation of the functional operation of the verification item in a controlled environment to yield qualitative results without the use of elaborate instrumentation or special test equipment.

d. Test. A procedure or action taken to determine under real or simulated conditions the capabilities, limitations, characteristics, effectiveness, reliability, or suitability of a material, device, system, or method.

Each segment level requirement will be tested and verified by one or more of these methods. A requirements matrix, mapping test cases to Level 4 requirements will include the method of verification. This matrix, mapping Release A segment level requirements to Release A test cases, is provided in Appendix B of this document.

3.3.2 Post Test Analysis

Post-test analysis includes data reduction and comparison of actual results against expected results. Any post test analysis required for CSMS I&T will be performed by the CSMS I&T organization with support from the user and development communities when appropriate. Methods for performing post-test analysis will be documented in the Segment/Element Integration and Test Procedures on a test by test basis. Post-test analysis will be documented in CSMS I&T reports. Data, data logs, event logs and any other test output required for post test analysis will be captured and stored under CM control.

3.3.3 Regression Testing

Regression testing is supplemental testing performed at any time upon any thread or build during CSMS I&T testing to ensure that existing software is not adversely affected by modified or new software. CSMS I&T members are responsible for planning, documenting, executing and reporting all regression testing. Automated test tools are used when practical, for regression testing by the CSMS I&T organization. This ensures that regression tests duplicate initial test procedures.

For Release A the following changes will result in regression testing:

- software changes
- hardware changes
- operational enhancements
- integration of two or more builds
- new versions delivered after the unit level testing

CSMS I&T organization is responsible for reporting any discrepancies encountered during segment regression testing. Discrepancies resulting from any other level of testing (i.e., System Test, Acceptance Test) which results in modifications at the unit level, will be regression tested at the segment level by the CSMS I&T organization.

3.3.4 Verification Resources

The following paragraphs in this section introduce and identify the resources necessary to accomplish CSMS I&T activities. Included are identification of test location and hardware and software configurations. Also discussed are the use of automated test tools, discrepancy reporting, and the role of CM in CSMS I&T activities.

3.3.4.1 Testing Facilities

The ECS Development Facility (EDF), located at the ECS facility in Landover, Md., has been designated as the testing facility for CSMS I&T activities. All CSMS Segment-Level test activity will take place at this location. This facility will be shared by the Segment Integration and Test personnel, Systems Integration and Test organization, the Independent Acceptance Test Organization and some developers. The test facility will be set up to emulate a DAAC or the EOC and will be re configurable to emulate the different functionality at each of the relevant DAACs. The facility will also have the capability to replicate, as close as possible the interfaces that will exist in Release A (e.g., DAAC to DAAC, SCF to DAAC, etc.) ECS will be solely responsible for the test environment. This includes installation, initial checkout and startup, upgrades/version control, access control and maintenance.

3.3.4.1.1 Hardware Items

The hardware CIs for the Release A time frame will be configured, as closely as possible (with the available EDF I&T hardware) to emulate the various DAACs and the EOC. The hardware will also be used to emulate all communications interfaces available for Release A, as closely as possible.

3.3.4.1.2 Software Items

For a complete listing of Build/Threads mapped to test cases, please see Appendix C.

3.3.4.2 Test Tools and Test Data

The CSMS I&T organization uses test tools for test development, test execution, and test management. Whenever possible test tools from the unit development and unit test environment are used. Additional test tools are COTS products or are developed by the Segment I&T organization. For a complete listing and description of the test tools please see Appendix A. For all test case which require an interface with SCF, ADC and various Users, the interfaces will be simulated. In all cases where testing of the DAACs is mentioned, we are referring to the ECS deployed facilities.

During CSMS test development, test tools will be used to develop test scripts and requirements to test cases. The CSMS I&T organization will use the ECS selected tools for test script development and requirements traceability. The ECS selected capture/playback tool to be used to develop test procedures. The ECS selected Requirements & Traceability Management (RTM) tool will be used for mapping CSMS I&T test cases to Level 4 requirements. This tool is used for all releases. A unique number is assigned to each build/thread and test case. This number is then used to identify the build/thread test case in RTM. The format for this identification number is consistent throughout all test organizations within ECS. The format is (B/T), for build or thread, (S/C/F/X/A), S - SDPF, C - CSMS, F - FOS, X - SI&T and A - IATO, (xxx) - representing the

build/thread number and (xxx) representing the test case number within that build. An example of this would be TC001.001.

During CSMS test execution, test tools will be used to simulate data and interfaces, decipher and monitor the data transmitted over the network and facilitate the execution of test procedures. Data interface simulators and user emulators are needed for interfaces that do not yet exist or are not yet mature enough for test use. Test data generators to simulate various data transmissions may be required. Additional tools for test execution include: capture playback tools, drivers, interface simulators, user emulators and data generators. A Network Analyzer will be used to collect and analyze the traffic that is transmitted over the network. Capture Playback Tools are used for replaying user sessions for regression testing, and to emulate multiple virtual sessions for system load and performance tests.

Test management tools record test results and aid in test result data analysis. These tools include loggers and other recording devices and reduction and analysis programs. File comparison utilities may be needed to compare data output with data input. A data reduction utility is needed to reduce large amounts of output data, such as output data from the PGS, to some meaningful evaluation of the data quality. The history log and systems logs gathered by CSMS systems management tools and agents will be used to aid in the data analysis phase of testing.

The capture playback tool selected was XRunner and the user emulation tool selected was LoadRunner. Both of these tools were developed by Mercury Interactive Corporation. The selection is defined in the EDS/ECS Source Evaluation Recommendation for Automated Test Tool Procurement (RFP #013). Hewlett Packard's OpenView is the selected Enterprise Management Framework that will be used to monitor the network activity, loads, etc. during the testing phase. The selection is documented in the EDS/ECS Source Evaluation Recommendation for Enterprise Management Framework (July 22, 1994).

Since there is no operational data available for Release A testing, test data is either provided from organizations holding appropriate data (i.e., TSDIS) or must be provided by a data generator. As ECS matures in future releases, the types and formats needed to satisfy test case needs will differ. Test data needed for Release A will be provided in Appendix A of this document.

Specific test tools and test data needed for Release A CSMS I&T will be identified as test cases, developed and documented in Appendix A of this document.

3.3.4.3 Discrepancy Reporting and Resolution

CSMS is required to report any noncompliance to Level 4 requirements encountered during CSMS I&T activities. The CSMS I&T organization will use the ECS selected COTS tool for tracking non conformance. It is the responsibility of the CSMS I&T organization to assure that all testers are trained to use the Nonconformance Reporting and Corrective Action (NRCA) system. The CSMS I&T staff will have the proper authority and access to the NRCA tool before any CSMS I&T activities begin. It is the responsibility of each tester to properly enter all discrepancies encountered during testing into the NRCA system. Once the discrepancy is corrected, regression testing is done to make sure no new problems have been introduced by the fix. If necessary, the tester will develop additional tests to ensure the problem is satisfactorily corrected. Quality

Assurance representatives are responsible for audits to ensure reported non conformances are resolved and properly verified.

3.3.4.4 Test Items Under Configuration Control

ECS CSMS I&T test documents, software and hardware configurations under test, test data sets, and software and hardware tools used for testing are maintained by CM. CSMS I&T will use the ECS selected COTS tool for configuration management control. It is the responsibility of the CSMS I&T organization to train all testers to use the CM tool. The CSMS I&T staff will have the proper authority and access to unit tested components using the CM tool before any CSMS I&T activities begin. Unit-tested components entered in the CM system are accessed by the CSMS testers. These components are verified and integrated by the CSMS I&T staff. Verified segment threads and builds are entered into the CM system upon successful completion of CSMS I&T verification activities. These are made available to the System I&T test team. The responsibility to provide CM at the DAACs is a CSMS requirement. The CM tool selected for the DAACs (Clearcase) is the same tool that is used at the EDF. If any discrepancies (see Section 3.3.4.3) are found during CSMS I&T, CM tracks the product changes and versions that result from correcting discrepancies.

3.4 CSMS I&T Organizations Roles and Responsibilities

The CSMS I&T roles include the following test positions and their corresponding responsibilities.

Test Conductor - A CSMS I&T member to conduct test execution. This person is responsible for establishing a stable and well defined test configuration before testing takes place. This person is also responsible for collecting test outputs and recording test results. Any problems encountered during testing are entered into the NRCA System by the test conductor.

Test Participants - CSMS I&T members and members of the segment development organization to perform subsystem integration and support test execution. Other supporting organizations include Maintenance and Operations (M&O) and Configuration and Data Management (CM). The ECS maintenance and operations organization will support the test members in the installation and configuration of the test environment and will support the test team if any system faults are encountered during testing. This would include such instances as computer software or hardware failures which cause the test configuration to be corrupted. M&O will be responsible for reconfiguring the system as needed to continue testing. CM will provide a controlled environment for the storing and maintaining of information about the test environment including hardware, software and test tool environments. CM also stores and catalogs test documents and test input data and output data.

Test Witnesses - Individuals invited to directly observe test conduct. This will include members from the System I&T organization and the IATO as appropriate in support of System I&T and IATO testing.

Test Monitors - The Quality Assurance organization is responsible for reviewing test data, materials, and documentation. These individuals need not be present during test conduct.

3.5 CSMS I&T Release Testing

CSMS I&T verification activities occur for each ECS formal release. This presently includes four Releases (A to D) and an Interim Release (IR-1). All releases follow the same formal release development track, with two exceptions for IR-1. Verification for IR-1 does not include a separate Critical Design Review and Test Readiness Review (TRR). Acceptance Testing and IV&V are not performed for IR-1. For all other Releases, CSMS conducts a series of TRRs and ETRs (Element Test Review).

TRRs are informal reviews conducted incrementally as portions of the CSMS are unit tested. As software units for each Release are developed and unit tested, informal TRRs are held to determine if the software units are ready for integration and test. Test procedures are reviewed at each TRR to determine if they are complete. If the software and test procedures are deemed ready, the CSMS I&T organization integrates and tests the software.

ETRs are informal reviews conducted incrementally as portions of the CSMS are integrated and tested. Each ETR reviews the results of the portion of the CSMS just integrated and tested. The reviews ensure that components are properly integrated and that segment level requirements are met.

When all CSMS software is developed and successfully integrated and tested, and informal TRRs for a Release are completed, a formal TRR is conducted to determine test readiness of the whole CSMS segment for that Release. A final, formal ETR is held to review the results of all integration and test activities held for the CSMS for that Release. After the final ETR, CSMS software is delivered to System I&T for integration with other segment software.

3.6 CSMS I&T Schedule Overview

3.6.1 Release Schedule

The following table (Table 3.6-1) shows CSMS I&T organizations activities across all ECS Releases. Program releases are indicated in the left most column of the chart. Program milestones are indicated across the top of the chart. For each release, CSMS I&T activities performed for each milestone are indicated. Dates for the milestones can be found in the ECS Release Plan (ECS document number 307/DV2).

Table 3.6-1. CSMS I&T Release Schedule (1 of 2)

Release	PDR/IDR	CDR	TRR	ETR	CSR
IR-1	- produce IR-1 CSMS I&T Plan (DID 319)		N/A	- conduct ETR upon completion of each segment level thread/build for IR-1 - conduct a final ETR for entire segment for IR-1	- IR-1 CSMS I&T Reports (DID 324/DV3)
A	- produce Release A CSMS I&T Plan (DID 319)	- produce Release A CSMS I&T Procedures (draft) (DID 322/DV3)	- conduct TRR upon completion of all unit development for Release A - produce Release A CSMS I&T Procedures (DID 322/DV3)	- conduct ETR upon completion of each segment level thread/build Turnover to the system test organization for Release A - conduct a final ETR for entire segment for Release A	- Release A CSMS I&T Reports (DID 324/DV3)
B	- produce Release B CSMS I&T Plan (DID 319)	- produce Release B CSMS I&T Procedures (draft) (DID 322/DV3)	- conduct TRR upon completion of all unit development for Release B - produce Release B CSMS I&T Procedures (DID 322/DV3)	- conduct ETR upon completion of each segment level thread/build Turnover to the system test organization for Release B - conduct a final ETR for entire segment for Release B	- Release B CSMS I&T Reports (DID 324/DV3)

Table 3.6-1. CSMS I&T Release Schedule (2 of 2)

Release	PDR/IDR	CDR	TRR	ETR	CSR
C	- produce Release C CSMS I&T Plan (DID 319)	- produce Release C SDPS I&T Procedures (draft) (DID 322/DV3)	- conduct TRR upon completion of all unit development for Release C - produce Release C CSMS I&T Procedures (DID 322/DV3)	- conduct ETR upon completion of each segment level thread/build Turnover to the system test organization for Release C - conduct a final ETR for entire segment for Release C	- Release C CSMS I&T Reports (DID 324/DV3)
D	- produce Release D CSMS I&T Plan (DID 319)	- produce Release D CSMS I&T Procedures (draft) (DID 322/DV3)	- conduct TRR upon completion of all unit development for Release D - produce Release D CSMS I&T Procedures (DID 322/DV3)	- conduct ETR upon completion of each segment level thread/build Turnover to the system test organization for Release D - conduct a final ETR for entire segment for Release D	- Release D CSMS I&T Reports (DID 324/DV3)

3.6.2 CSMS I&T Scheduling for Release A

Since the specific schedule may change, please see the scheduling information located in the ECS Intermediate Logic Network (CDRL 194-108-MG2) to determine exact dates. The individual threads and builds as documented in the Build/Thread Plan (Figure 3.2-1) are also in the ECS Intermediate Logic Network with specific dates. For a general schedule of the CSMS I&T for Release A please see the timeline at the bottom of Figure 3.2-1 (this will show the duration planned to test each build/thread, but not the specific date the test will occur).

4. CSMS Release A Test Descriptions

The following sections identify the segment level threads and builds used in Communications and Systems Segment Integration and Test for Release A (shown in Figure 3-2.1). First, threads are identified. Threads are the aggregation of unit tested components (CSCIs, CSUs, COTS software). Each thread demonstrates a CSMS function. Builds are the integration of threads and are identified after each series of threads which make up a build. Test cases are identified for each thread and build. The primary objective of each test case is to demonstrate and verify the capabilities of each function as stated in Level 4 requirements. All CSMS thread and build test cases will be conducted at the Landover EDF (see Section 3.3.4.1, Testing Facilities).

4.1 Internetworking Thread Test (TC017)

This thread tests the Internetworking infrastructure for Release A. Internetworking consists of the Physical, Data Link, Network, and Transport layers of the OSI Reference Model. Internetworking includes the LANs at the DAACs, the ESN WAN provided by PSCN, and interfaces to external networks. Release A interfaces are shown in the following table. The interfaces with asterisks were tested in IR-1.

Table 4.1-1. Release A Interfaces (1 of 2)

Physical Interface (From)	Physical Interface (To)	Function	Data	Network & Comments
*GSFC SDPF	ECS MSFC DAAC	Process LIS level 0 data	Level 0, Q/L, Definitive and Predicted Orbits	NOLAN (WAN)
*GSFC SDPF	ECS LaRC DAAC	Process CERES level 0 data	Level 0, Q/L, Definitive and Predicted Orbits	NOLAN (WAN)
*GSFC DAAC	GSFC TSDIS	VIRS products reprocessing of GSFC DAAC archived data	Archived Level 1A-3 data products, Metadata, browse, algorithms, documentation and ancillary	Exchange LAN
*MSFC DAAC	LIS SCF	Processed Q/L to LIS SCF, Algorithm I&T data	Processed Q/L data, AI&T results data	MSFC Campus Network
*LaRC DAAC	CERES SCF	Processed Q/L to CERES SCF, Algorithm AI&T data	Processed Q/L data, AI&T results data	LaRC Campus Network
*GSFC MOC	MSFC SCF	Remote displays related to LIS operations at MSFC	Support for LIS project operations	NOLAN (WAN)

Table 4.1-1. Release A Interfaces (2 of 2)

Physical Interface (From)	Physical Interface (To)	Function	Data	Network & Comments
*GSFC MOC	LaRC SCF	Remote displays related to CERES operations at LaRC	Support for CERES project operations	NOLAN (WAN)
*GSFC MOC	GSFC TSDIS	Remote displays related to PR, TMI, VIRS production data sets	Support for real time instrument operations	As Applicable
*GSFC SDPF	GSFC TSDIS	For processing L0 data at TSDIS for PR, TMI, and VIRS	Level 0, Q/L & Definitive Orbit Data (via SDPF from FDF)	As Applicable
*LIS SCF	MSFC DAAC	For Algorithm I&T LIS	Science Algorithms, test data, documentation	MSFC Campus Network
*CERES SCF	LaRC DAAC	For Algorithm I&T CERES	Science Algorithms, test data, documentation	LaRC Campus Network
*NOAA	GSFC	Ancillary data for LIS & CERES product processing	Ancillary data and metadata	ESN(V0) Via Suitland
*EDF Landover	GSFC, LaRC, MSFC, EDC DAACs	Software CM, Systems Management	ECS COTS and Custom Software Builds, Status	ESN(V0) All entities interconnected
*EDC	JPL	Aster AI&T	Algorithms and related data	ESN(V0) JPL Campus Network
GSFC, LaRC, MSFC, EDC	External Users	E-mail, FTP, Telnet	Data Requests, E-mail, Data products	NSI
ESN Wan(ISS)	International Partners	Telnet	Command requests, data requests, products	ESN
EDC DAAC LAN	EDC External Users	EDC External User Interface	Data Requests, Data products	EDC Campus LAN
EDC DAAC LAN	Landsat Production System	Landsat 7 data ingest	Landsat 7 data	Landsat Production System Network
EOC LAN	EDOS	Satellite and Instrument command and telemetry	Satellite and Instrument command and telemetry	Ecom
EOC LAN	IST's	interface testing	Command requests, telemetry	ESN
EOC LAN	IST at Goddard	interface testing	Command requests, telemetry	Exchange Lan
GSFC DAAC LAN	Color external users on GSFC Exchange Network	interface testing	test data	Exchange LAN

* Tested in IR-1

Special resources required for this thread include:

- XRunner
- LoadRunner
- HP OpenView Network Management
- Network analyzer

- Internetworking benchmark test suite
- Standard bodies Inter networking test results
- External Interface Simulators and Emulators
- External Interface test data

This thread contains 5 test cases.

4.1.1 Test Case 1: External Interfaces IR-1 Regression Test (TC017.001)

This test case regression tests the External interfaces previously tested in IR-1 (shown with asterisks in the external interface table). IR-1 interface tests are described in Volume 1, Section 4.1 of the CSMS Segment I&T Plan.

4.1.2 Test Case 2: Internetworking IR-1 Regression Test (TC017.002)

This test case regression tests the Internetworking functionality tested in IR-1. IR-1 Internetworking tests are described in Volume 1, Section 4.2 of the CSMS segment I&T plan.

4.1.3 Test Case 3: Release A Interface Test (TC017.003)

These tests will attempt to demonstrate that the interfaces described above will function properly and that test data representative of the required data can be successfully transmitted or processed. Other interfaces tested include: V0 WAN and the MSFC, LaRC and GSFC DAACs for the purpose of IR1 interface testing and with NSI (or an alternate internet provider). The testing of the interfaces will take place at the EDF using emulation and simulation. In cases where it is technically, logically, and procedurally feasible and cost effective, the interfaces will be tested using actual facilities (i.e., NSI or ESN). Test drivers and logging will be used to performance test the interfaces.

Test Inputs

Benchmark interface test data

Test Steps

Run an XRunner script to interface with all of the entities outlined in the above table.

Verify that the ISS provides an interface between the V0 WAN and the MSFC, LaRC, and GSFC for IR-1 interface testing.

Demonstrate the capability of the ISS to interface with NSI or an alternate Internet provider at the GSFC, MSFC, LaRC and EDC to provide DAAC access to science users as outlined in the Communications and System Management Segment (CSMS) Requirements Specification for the ECS Project.

Test Outputs

Comparisons of input and output data, System Management logs including performance data, network analyzer outputs.

Success Criteria

The interfaces function properly, data is communicated reliably and accurately, performance results meet RMA requirements.

Assumptions and Constraints

None

4.1.4 Test Case 4: Release A Internetworking Test (TC017.004)

This tests case tests Internetworking services for TCP/IP over ethernet, FDDI, and HiPPI (if needed). The tests will be conducted in the EDF on facilities emulating Release A DAAC LAN's as closely as possible. The tests will include using controlled loads to evaluate network performance.

Test Inputs

Benchmark Internetworking test data.

Test Steps

Run Internetworking benchmark test suite.

Test Outputs

Comparisons of test data sent and received, network analyzer outputs, log data indicating performance and fault data, and network manager alarms.

Success Criteria

Data successfully transported through the network, performance data consistent with prior and standard benchmark results, no anomalous performance or fault log or alarm events.

Assumptions and Constraints

This functionality will be further verified in other build/thread tests since Internetworking will be a part of most other tests.

4.1.5 Test Case 5: Network Filtering Test (TC017.005)

This test demonstrates the Internetworking filtering of packets on port/socket and/or source and/or destination address. This test will be conducted in the EDF on facilities that emulate Release A as closely as possible.

Test Inputs

Router configurations establishing filtering conditions. Test packets with combinations of port/socket identification and source/destination addresses.

Test Steps

Run telnet, remote log on, file transfer, and interprocess jobs that create the above described test packets.

Test Outputs

Network management logs showing the success or failure of the various packets in getting through the Internetworking filters.

Success Criteria

Not allowed packets fail, allowed packets passed. Log records of failed packets.

Assumptions and Constraints

This functionality will be further verified in other build/thread tests since Inter networking will be a part of most other tests.

4.2 Graphical User Interface (GUI) Thread Test (TC018)

This thread will demonstrate and test all CSS, COTS and custom GUIs, respectively. The GUIs tested herein represent multiple functionality and services related to the CSS tasks implemented in Release A.

This thread has the function of providing a graphical user interface for the following applications:

* Telnet - during a remote login (virtual terminal)
* Tools - during the M&O of DCE services, File Access and Transfer, Bulletin Board, etc.

The objective of this test is to verify that the CSS Common Facilities provide a standard GUI that can be used for remote GUI based sessions from various platforms, as well as users within and without the ECS domain.

Special resources required for this thread test include:

- XRunner
- Operational DCE cell
- Host workstations with X-window capability
- Simulated access to workstations at DAACs, SCFs, and External ECS Users

This thread contains 3 test cases:

4.2.1 Test Case 1: Secure Virtual Terminal (TC018.001)

The purpose of the Secure Virtual Terminal test is to verify that client server terminal interaction can be handled through a virtual device with common capabilities, thus hiding the underlying terminal characteristics from the user. This capability is provided to DAAC and SCF users within the ECS domain through a secured virtual terminal service (ktelnet).

Test Inputs

There are no special inputs to this test.

Test Steps

1. login to local DAAC host
2. telnet over to a remote DAAC host
3. verify that current terminal allows access to remote DAAC host (directories, files, etc.)
4. verify that the means to enhance characteristics of the basic virtual device by mutual agreement between the two communicating parties
5. verify that the virtual terminal is capable of supporting octet
6. logout of remote DAAC host
7. repeat steps 1 through 4 for the following combinations:

   SCF to DAAC

   DAAC to SCF

   SCF to SCF

Test Outputs

The expected results of this test include terminal sessions to remote DAAC/SCF hosts.

Success Criteria

This test will be deemed successful when users will be able to connect through remote virtual terminal sessions to DAAC and SCF hosts.

Assumptions and Constraints

None.

4.2.2 Test Case 2: Unsecure Virtual Terminal (TC018.002)

The purpose of the Unsecure Virtual Terminal test is to verify that client server terminal interaction can be handled through a virtual device with common capabilities, thus hiding the underlying terminal characteristics from the user. This capability is provided to users outside of the ECS domain through a non-secured virtual terminal service (telnet).

Test Inputs

There are no special inputs to this test.

Test Steps

1. login to external host
2. telnet over to a remote DAAC host
3. login to the ECS guest server, as a non-registered user, with guest access

4. verify that current terminal allows access to remote DAAC host (directories, files, etc.)
5. logout of remote DAAC host
6. repeat steps 1 through 4 for the following combinations:

   DAAC to external host

   external host to external host

   SCF to external host

   external host to SCF

Test Outputs

The expected results of this test include terminal sessions to remote DAAC/external hosts.

Success Criteria

This test will be deemed successful when users will be able to connect through remote virtual terminal sessions to DAAC, SCF and external hosts.

Assumptions and Constraints

None.

4.2.3 Test Case 3: Common Facility GUI Based Sessions (TC018.003)

The purpose of the Common Facility GUI Based Sessions test is to demonstrate the graphical user interface for the various tools provided with the CSS Common Facilities and Services.

Test Inputs

There are no special inputs to this test.

Test Steps

1. Startup the following COTS GUI services:

   E-Mail

   Bulletin Board

   File Access and Transfer

   DCE operations (cdscp, rgy_edit, dtscp, etc.)
2. Demonstrate functionality provided through the use of these GUIs for the Common Facilities

Test Outputs

The expected results of this test include successful demonstration of CSS Common Facilities and Services.

Success Criteria

This test will be deemed successful if all CSS Common Facilities and Services operate through GUIs.

Assumptions and Constraints

None.

4.3 Directory/Naming Service Thread Test (TC019)

The purpose of this thread is to verify the functionality of the Directory/Naming Service, which is used to uniquely associate a name with resources/principals along with their attributes. This thread includes the regression testing (IR-1 functionality) of those Directory Service functions dealing with standard X/Open functions, replication, and distribution, as well as the added Release A capability dealing with defining attributes and Extensibility.

Special resources required for this thread test include:

- DCE cell(s)
- Cell Directory Service Command Program (cdscp)
- Custom X/Open commands
- X.500
- Domain Name Services (DNS)

This thread contains 3 test cases.

4.3.1 Test Case 1: Directory/Naming Service Regression Testing (TC019.001)

This test case regression tests IR-1 Directory/Naming Service capability. Regression testing will include:

1. X/Open Functions
2. Replication
3. Distribution (verify that the directory service maintains multiple copies of the namespace on different hosts to provide fault tolerance)

A description of this testing is contained in Section 4.4 of Volume 1 of the CSMS I&T Plan.

4.3.2 Test Case 2: Attributes (TC0019.002)

This test case will demonstrate that the Directory/Naming Service can facilitate the function of permitting application users to define attribute schema for various services.

Test Inputs

APIs to perform X/Open functions.

Test Steps

Log onto an ECS deployed site workstation.

Ensure that there are at least 20 unique object IDs obtained from standard bodies (listed in standard header files).

Define a property schema for a DB entry.

Enter attribute value pairs for that schema.

List the newly defined attribute pairs for that schema.

Test Outputs

The Directory/Naming Service should display all attribute types and attribute pairs for defined schema.

Success Criteria

The Directory/Naming Service should provide at least 20 unique object IDs for the application programmer to use.

Assumptions and Constraints

None.

4.3.3 Test Case 3: Extensibility (TC019.003)

This test case will demonstrate that the Directory/Naming Service can provide a mechanism to communicate with X.500 and DNS standard name services for name resolution.

Test Inputs

cdscp commands

Test Steps

Log onto an ECS deployed DAAC server workstation.

Using cdscp commands, request information stored in a X.500 directory.

Using cdscp commands, request information stored in a foreign cell's local namespace, connected via DNS.

Demonstrate the functionality of the Directory Service to provide multiple agents which cooperate among themselves through referral and chaining to perform directory operations.

Test Outputs

The Directory/Naming Service should return the requested information.

Success Criteria

This test will be deemed successful when the Directory/Naming Service enables one to communicate with the X.500 and DNS naming services.

Assumptions and Constraints

It is assumed that the file system will be populated with a number of directories, sub directories, data files, and other objects across the X/Open, X.500, and DNS name services.

4.4 Distributed File Service Thread Test (TC020)

This thread has the function of providing file transfer and file management capabilities through interactive access and application interfaces across a distributed environment.

The objective of this test is to verify that DFS provides a transparent interactive and non-interactive file transfer capability, as well as transparent remote file access.

Special resources required for this thread test include:

- LoadRunner / XRunner
- Operational DCE cell
- APIs for file transfer and Remote File Access
- Simulated access to workstations at DAACs, SCFs, and External ECS Users

This thread contains 4 test cases:

4.4.1 Test Case 1: Interactive File Transfer (TC020.001)

The purpose of the Interactive File Transfer test is to regression test the file transfer capabilities in IR-1.

Test Inputs

Inputs to this test case include ASCII/Binary files representative of the science data products available in Release A.

Test Steps

1. logon to local DAAC host
2. ftp files to local DAAC host
3. verify (via checksum) that files on both ends match
4. ftp files to remote DAAC host
5. verify (via checksum) that files on both ends match
6. simulate transferring files to SCF host via ftp
7. verify (via checksum) that files on both ends match
8. ftp files to external host
9. verify (via checksum) that files on both ends match

Test Outputs

The expected results of this test include matching checksums for files on both send and receive ends.

Success Criteria

This test will be deemed successful when all file checksums are identical.

Assumptions and Constraints

DAAC refers to the ECS deployed software at each site.

4.4.2 Test Case 2: Non-Interactive File Transfer (TC020.002)

The purpose of the Non-Interactive File Transfer test is to verify that files can be sent through a scheduling option without user presence.

Test Inputs

Inputs to this test case include ASCII/Binary files representative of science data products available in Release A.

Test Steps

1. logon to local DAAC host
2. ftp series of files to local DAAC host
3. verify that files are transferred without user presence (scheduled by the file transfer service utilizing file transfer APIs)
4. verify (via checksum) that files on both ends match
5. repeat steps 2 through 4 for the following combinations:

   DAAC to SCF

   DAAC to external host
6. repeat steps 2 through 4 while injecting a file transfer failure
7. verify that the proper events were logged and alarms sent

Test Outputs

The expected results of this test include matching checksums for files on both send and receive ends.

Success Criteria

This test will be deemed successful when all file checksums are identical and alarms are sent whenever scheduled operations fail.

Assumptions and Constraints

DAAC refers to the ECS deployed software at each site and all interfaces to SCF and external hosts will be simulated.

4.4.3 Test Case 3: Remote File Access (TC020.003)

The purpose of the Remote File Access test is to verify that remote files can be accessed as if they were part of the local file system.

Test Inputs

There are no special inputs to this test.

Test Steps

1. logon to local DAAC host
2. rlogin to remote DAAC host
3. traverse directories and access specific files (both interactively and through the use of remote file access APIs)
4. verify that remote files are transparently accessed on the remote host within the set user privileges and access controls

Test Outputs

The expected results of this test include user ability to access remote files from a local host.

Success Criteria

This test will be deemed successful when all remote files can be accessed within the set user privileges and access controls.

Assumptions and Constraints

It is assumed that the file system will be populated with a number of directories and files. DAAC refers to the ECS deployed software at each site. If the ECS software is not readily available this activity will be simulated.

4.4.4 Test Case 4: File Transfer Scheduling (TC020.004)

The purpose of File Transfer Scheduling test is to verify the functionality associated with the CSS File Access Service.

Test Inputs

Scheduling of a batch mode file transfer, noninteractive operations to operator specific log files and initialization of alarms and events.

Test Steps

Verify the ability to schedule file transfers in batch mode.

Initialize a noninteractive operation, verify that the results of the operations shall log results to operator specified log files.

Fail a scheduled operation, verify that the File Access Service provides an option to send alarms and generate events.

Test Outputs

Log files with the appropriate information indicating successful file transfers, and alarms Generated events when a scheduled operation failed.

Success Criteria

This test will be deemed successful when all of the related File Access Service has been demonstrated and/or tested and verified.

Assumptions and Constraints

None.

4.5 E-Mail/Bulletin Board Service Thread Test (TC021)

The purpose of this thread is to test the Electronic Mail message management capability and the network Bulletin Board Service's capacity to provide a forum for sharing ECS related information. The BBS management interface will be tested to demonstrate the following functions for authorized ECS users:

a. creating new BB
b. deleting existing BB
c. deleting messages(s) from BB
d. backup BB(s)
e. force users off a single BB or entire system for backup
f. collecting access history and/or statistical information

The BBS will be tested to demonstrate on-line help, and for having an interface to E-mail, whereas users can respond to a message on a bulletin board by sending a response to the author only or by posting a message to one or more bulletin boards. The BBS must demonstrate hypertext links capability and a feature for "WHAT's NEW", which informs the user of new information available on the BBS.

Special resources required:

- DCE Cell
- SMTP/X.400 protocols
- Multi-purpose Internet Mail Extensions (MIME)
- XRunner
- Usernet BBS via XRN interface

This thread contains 6 test cases.

4.5.1 Test Case 1: General E-MAIL Messaging (TC021.001)

The general E-Mail messaging test will demonstrate the capability of the electronic mail messaging function to exchange messages across external mail systems based on SMTP and X.400 protocols, by sending and receiving the Multi-purpose Internet Mail Extension (MIME) messages available at GSFC, which supports X.400 operations. This test verifies the translation between SMTP and X.400, through interactive and non-interactive service modes.

This test will also demonstrate the E-Mail capability to auto respond to messages being received by the DAAC, and demonstrate E-Mail capacity to send specific replies to a received message either to the author only or to all destinations addressed in the incoming message.

Test Inputs

Test input requires creating two simple mail messages. One will include a message designed to generate an automatic response from the receiving DAAC, which responds only to the author of the message. The second message is designed to distribute an automatic response from the receiving DAAC to a list of destinations, listed in the incoming message. These messages will be sent across the external mail system which is configured with the required protocols for this test.

Test Steps

Author Only

1. Create an E-Mail message which requires an automatic response to the author only.
2. Send message to DAAC.
3. Verify receipt of proper E-Mail response and destination.

Distribution Lists

1. Create an E-Mail message which requires an automatic response to distribution list.
2. Send message to DAAC. [GSFC]
3. Verify receipt of proper E-Mail response and destinations.

Test Outputs

The expected results of this test include successful message transfers across the external mail system along with the required automatic responses, as defined in this test.

Success Criteria

When all validation and verification of all messages transferred or received have been determined to have satisfied the overall test requirements.

Assumptions and Constraints

All required network configurations and E-Mail messaging features are properly configured. DAAC refers to the ECS deployed software at each site. If the ECS software is not readily available this activity will be simulated.

4.5.2 Test Case 2: E-MAIL Mailtool (TC021.002)

The E-Mail Mailtool test will demonstrate the capability of the messaging service to manage and interact with user E-mail.

Test Inputs

Test input requires creating a user defined MAILBOX which will store incoming messages in the mailbox folders, created for long term archiving. This mailbox will be tested for, copying and/or moving messages from the MAILBOX to the user defined folders, and for providing an access control feature which requires authentication for access to the Mailtool via login and password. The MAILBOX will also be tested for allowing users to set an automatic time period for deletion of messages to help manage the MAILBOX size, by removing old messages after confirmation. A summary status for all mail messages will be verified to determine the inclusion of the following:

a. title/subject

b. name of the Author

c. date/time message received

d. show whether message was read

The message editor will be tested for the capability of composing messages, by providing a title/subject field for the message.

The service must allow for destinations of the following types:

a. single user

b. position managed by one or more users

c. site which consist of several users

d. bulletin board

This E-Mail service will be tested for the capability of maintaining either public or private mailing lists or both.

Following is a list of MAILBOX features to be verified and tested:

1. attaching files to a message
2. discarding message(s) without saving
3. forwarding messages
4. perform cut/copy/paste/delete/undo operations from editor
5. select Next or Previous messages in the MAILBOX or selected folder
6. search keywords in messages
7. search MAILBOX or folders for keywords in the title text

Test Steps

1. Mailbox Copy/Move verification
2. Mailbox Authentication verification
3. Automatic deletion verification
4. Summary status information
5. Message editor verification
6. Mailbox feature verification

Test Outputs

The expected results of these tests are a successful demonstration of all the required interactive user functions provided by the MAILBOX and folder. Validation and verification of each test must be complete and satisfactory.

Success Criteria

When all validation and verification of all Mailtool functions have been determined to have satisfied the overall test requirements.

Assumptions and Constraints

None.

4.5.3 Test Case 3: E-MAIL API (TC021.003)

The E-Mail API test will demonstrate the capability of the E-Mail service to provide non-interactive messaging services.

Test Inputs

Test input requires an API to be written to demonstrate the capability to send an E-Mail message programatically. The message sent must have multiple files attached to it and have the file name as input for the message text. This message along with the attachment will then be sent to multiple destinations, including a bulletin board, and the E-Mail service must accept the mailing list as valid destinations.

Test Steps

Create an XRunner script that will attach multiple or binary files to a newly created mail message which contains the message filename as message text input This message along with the attachment will then be sent to multiple destinations including a bulletin board.

Test Outputs

The expected results of these tests are a successful demonstration of all the required non-interactive user functions provided by E-Mail API. Validation and verification of each test must be complete and satisfactory.

Success Criteria

When all validation and verification of all API functions have been determined to have satisfied the overall test requirements.

Assumptions and Constraints

All required API features are properly developed.

4.5.4 Test Case 4: General Bulletin Board Service [BBS] (TC021.004)

The General BBS test will demonstrate the capability of the BBS service to provide a forum for sharing ECS related information on the required platforms the service must support.

Test Inputs

Test inputs require the following protocol standards to be configured:

- SMTP protocols
- NNTP
- TCP/IP
- Usenet message standard (RFC 850)

Test Steps

1. Bringup the USERNET news system via xrn interface.

User Login to BBS

2. Execute XRunner script to login 100 users.

Messaging and File transfer

3. Verify multiple messages posted for various bulletin boards.
4. Verify multiple bulletin boards accessed via xrn interface.
5. Create a new bulletin board message and annotate an audio file and a video file within the message.

Security/Access Control

6. Access a secured bulletin board from the BBS service and verify that user registration is required.
7. Login to the secured bulletin board.
8. Create a file with specified permissions, which grant only authorized users access to the file.
9. Attempt to access the transferred file, with and without the appropriate access controls.
10. Verify the access controls transferred with the file.

Statistical report of the access history

11. Create a statistical report of the access history which includes the following information:
    a. each user
    b. system login count
    c. total time on-line
    d. total time for downloads
    e. messages read status for each BBS
    f. each BBS
    g. message count
    h. ast cleanup
    i. last backup
    j. access count

Toolkit Distribution

12. Create an ECS toolkit distribution list.
13. Distribute toolkit.
14. Verify toolkit distributed properly.

Management Interface

15. Using the BBS management interface execute the following functions:
    a. creating new BB
    b. deleting existing BB
    c. deleting messages(s) from BB
    d. backup BB(s)
    e. force users off a single BB or entire system for backup
    f. collecting access history and/or statistical information
16. Verify all functions listed function properly.

Online-Help

17. Access the online-help facility.
18. Verify help function is accurate.

BBS E-Mail Interface

19. Create a message reply response to the author of a bulletin board message.
20. Post a message response to multiple bulletin boards.
21. Post a message response to a single bulletin boards.

What's New

22. Access BBS news update feature.
23. Explore the hyperlink sublevels.

Test Outputs

The expected results of these tests are a successful demonstration of the capability of the BBS service to provide a proper forum for sharing ECS related information on the required platforms and interactive functions. Validation and verification of each test must be complete and satisfactory.

Success Criteria

When all validation and verification of all BBS functions have been determined to have satisfied the overall test requirements.

Assumptions and Constraints

BBS service available to ECS users. Depending on availability moderated and/or non-moderated. The BBS must demonstrate the capability to provide both moderated and non-moderated bulletin boards that will support up to 1000 bulletin boards and provide concurrent access to as many as 100 users. The BBS will be tested for allowing multiple messages for each bulletin board and the capability of supporting audio and video annotations in the bulletin board messages. User registration will be demonstrated, along with the capability to transfer files and control file access, to files designated to grant only authorized users access to the file. BBS must demonstrate ECS tool kit distribution. Access history and statistical information must be maintained for the following :

a. each user
b. system login count
c. total time on-line
d. total time for downloads
e. messages read status for each BBS
f. each BBS
g. message count
h. last cleanup
i. last backup
j. access count

4.5.5 Test Case 5: Mailtool Bulletin Board Service (TC021.005)

The BBS Mailtool test will demonstrate the capability of interactive functionality for any bulletin board user. The bulletin board will be tested for the capability of users to either subscribe or unsubscribe to any bulletin boards and to select a subscribed bulletin board for viewing all messages in that bulletin board. The capability of the bulletin board to respond to a message by

sending the response to the bulletin board and/or to the author and/or any other user specified destination, will be tested.

The following search capability will be tested for bulletin board users:

a. search for a string in message headers and in message text

b. search by author

c. search by subject

A catch-up feature which excludes user specified messages from appearing in the bulletin board when it is viewed next time, will be tested. The bulletin board services must demonstrate that users can post messages to bulletin board(s), maintain an access history for each bulletin board per user basis, which tracks the messages read by the user for each bulletin board. Saving messages to the local bulletin board system will be tested, along with attaching ASCII or binary files to a message being sent. Also, a means to retrieve files will be tested.

The BBS must demonstrate the following bulletin board configuration options:

a. screen size

b. number of messages displayed on a screen

c. screen colors (background/foreground)

d. read message indicator

Test Inputs

Sequence of interactive commands simulating BBS usage for search, configuration, message retrieval, etc.

Test Steps

Copy files from the BB.

Demonstrate the functionality of the Bulletin Board Service to collect and maintain access history.

Inspect the statistical information for the service.

Verify that you can access the Bulletin Board Service in interactive mode from the command line.

Subscribe and unsubscribe to the BB through the Bulletin Board Service.

Select a subscribed BB to view summary information of all the messages within that BB.

Respond to a message specifying the destination.

Demonstrate the capability to perform a search by various topics (i.e., author, subject).

Demonstrate the functionality of the catch-up feature.

Verify that you can save/copy a message to the local system.

Test the interface that exists to allow applications to post a message to the bulletin board.

Test Outputs

The expected results of these tests are a successful demonstration of the capability of the BBS service to provide interactive functions to BBS users. Access history, statistical information, subscribed and unsubscribed bulletin boards, response to a message, a search, users specified messages excluded the next time that BB is viewed, copy of the message, and an application interface with the BB. Validation and verification of each test must be complete and satisfactory.

Success Criteria

When all validation and verification of all BBS functions have been determined to have satisfied the overall test requirements.

Assumptions and Constraints

BBS service available to ECS users. That the interface between the BB and application is already in place.

4.5.6 Test Case 6: API Bulletin Board Service (TC021.006)

The BBS API test will demonstrate the capability of the BBS service to provide non-interactive BBS services for programmatic interface functions.

Test Inputs

Test inputs include demonstrating the capability of the BBS service to provide a programmatic interface to post a message to a bulletin board and to have a message posted to multiple bulletin boards. Also, BBS will be tested for attaching ASCII and binary files to a message.

Test Steps

Verify that a user can post a message to a bulletin board(s).

Verify that a user can copy and/or save a message to his local system.

Demonstrate the capability to attach an ASCII or binary file to a message.

Test Outputs

The expected results of these tests are a successful demonstration of the capability of the BBS service to provide non-interactive functions to BBS users. Validation and verification of each test must be complete and satisfactory. A copy of a message on the BB saved/copied to a users local system. A message posted to the BB with an ASCII or binary file attached to it.

Success Criteria

When all validation and verification of all BBS functions have been determined to have satisfied the overall test requirements.

Assumptions and Constraints

BBS service available to ECS users.

4.6 PGS Toolkit Interface Thread Test (TC022)

This thread has the function of providing a variety of interfaces to PGS Toolkits for the purposes of file access, event logging, time services, message passing, thread services, etc.

The objective of this test is to verify that CSS interfaces (namely APIs) are available for use by PGS Toolkits.

Special resources required for this thread test include:

- LoadRunner / XRunner
- Operational DCE cell
- Access to workstations at DAACs, SCFs, and External ECS Users

This thread contains 2 test cases:

4.6.1 Test Case 1: Common Facilities APIs (TC022.001)

The purpose of the Common Facilities APIs test is to verify that PGS Toolkit developers and users can utilize the APIs provided by the CSS Common Facilities.

Test Inputs

Inputs to this test case include PGS Toolkit drivers (simulating PGS related API calls), and CSS APIs.

Test Steps

1. execute PGS Toolkit driver script
2. CSS APIs will be called by the test driver
3. verify the appropriate outcome of the API call

Test Outputs

The expected results of this test include:

File Access API - verify that proper files (both local and remote were accessed and information was retrieved)

File Transfer API - verify that all designated files were transferred (verify checksums)

Event Logging API - verify that all designated events are logged in the appropriate history log

Success Criteria

This test will be deemed successful when all PGS Toolkit API calls result in the events detailed above.

Assumptions and Constraints

None.

4.6.2 Test Case 2: Object Services APIs (TC022.002)

The purpose of the Object Services APIs test is to verify that PGS Toolkit developers and users can utilize the APIs provided by the CSS Object Services.

Test Inputs

Inputs to this test case include PGS Toolkit drivers (simulating PGS related API calls), and CSS APIs.

Test Steps

1. execute PGS Toolkit driver script
2. CSS APIs will be called by the test driver
3. verify the appropriate outcome of the API call

Test Outputs

The expected results of this test include:

Event Services APIs - verify that asynchronous communications are supported between PGS Toolkit objects.

Verify that a push API and pull API exist. (push allows the supplier of events to initiate the transfer of event data to consumers, pull allows a consumer to request the event data)

Verify that multiple suppliers can communicate with multiple consumers without limiting the accessibility of the data.

Verify that the event data is passed as a parameter.

Test the CSS provided Event Service APIs to: verify that push and pull events will be terminated, verify that the suppliers and consumers are connected to an intermediary, block until the pull event data is available or an exception is raised, verify that a proxy is used to connect consumers and suppliers.

Time Service APIs - verify that PGS Toolkit processes can get the proper distributed time.

Lifecycle Service APIs - verify that PGS Toolkit processes are given the states and invocations.

Demonstrate the capability to create a new object for a client.

Test the APIs capability to accept resource preference information.

Demonstrate that a server is available to service a user request.

Verify during client/server connection phase the Lifecycle Service acts as an intermediary.

Thread Service APIs - verify that PGS Toolkit threads (as in UNIX threads) are synchronized when accessing shared data.

Test the functionality of the Thread Service APIs to provide a synchronizing object that is in one of two states: locked or unlocked. (verify that it locks the synchronizing object before it accesses the shared data and unlocks it when it is finished.)

Verify that each invocation of a server operation runs as a distinct thread.

Test the ability of the API to account for the possibility of other threads changing shared data at any point.

Success Criteria

This test will be deemed successful when all PGS Toolkit API calls result in the events detailed above.

Assumptions and Constraints

Assume APIs for the above are available. Note that Security Service, Message Passing, Time Service, and DOF Service APIs are tested in other threads.

4.7 Communications Services Build Test (BC023)

The Communications Services Build represents the integration of the CSS and ISS functionality for Release A. This test is an aggregation of the Internetworking, GUI Based Session, Directory Service, Distributed File Service, E-mail/Bulletin Board Service and PGS Toolkit Interface Threads, as well as the CSMS IR-1 Communications Build. The CSMS IR-1 Communications Build is an aggregation of the CSS and ISS functionality that carries over into Release A from IR-1. The functionality regression tested from IR-1 includes: file transfers, communication via the internet, ACLs and external interfaces. Release A functionality tested includes: multicasting, file access, virtual terminal and DCE enhancements.

The objective of this test is to verify that all of the previously tested functionality is still available upon integration of the Communications Build.

Special resources required for this thread test include:

- Sensor Data Processing Facility(SDPF) simulator
- TRMM Science Data and Information System (TSDIS) simulator
- NOLAN emulation, for example protocols
- Emulated IR-1 DAAC configuration
- HP OpenView
- Network analyzer
- NSI and ESN V0 connections
- XRunner

This thread contains 7 test cases.

4.7.1 Test Case 1: IR-1 Regression (BC023.001)

The purpose of the IR-1 Regression test case is to demonstrate that upon the integration of the ISS and CSS functionality from IR-1 the software will still function as expected in Release A. This functionality includes: communicating over a variety of interfaces, ability to transfer files from DAAC to DAAC to SCF to EDF and communication amongst the DAACs via E-mail.

Test Inputs

Inputs to this test case include various combinations of valid/invalid ID and valid/invalid password, valid admin ID and password, valid add, change and delete registry commands, ability to access and modify directories, time checks using DTS. RPC calls within a host and from host to host will also be tested. A file to be transferred and a composed E-mail message.

Test Steps

Verify which of the interfaces exist

Through simulation or use of non-operation IR-1 data, verify that the interfaces are functional

Run an XRunner script that calls a file with various valid/invalid IDs/passwords

Upon successful login, call another XRunner script to change the users password, logout and login with the new password

Logon as the DCE Administrator

Add, change, and delete commands to/from the security registry

Set up a cron job to retrieve the time from each of the workstations in the operational cell and store them in a file

Inspect the file to insure that all of the times are in sync

Set up a workstation to run as the server

Set up all of the workstations to be clients (including the server workstation)

Initialize the server

Initialize communications between client and server

Create a file equivalent in size to an SCFs algorithm

Using ftp transfer the file from SCF to each of the DAACs.

From the DAAC(s) return an E-mail message to the SCF verifying that the file has been received

Send an E-mail message between the DAACs (plus EDF), making sure that each site sends/receives at least one message

Test Outputs

Test outputs include data products/outputs produced by the emulation. Screen outputs showing the success or failure of the logon/logoff attempts. Response times of each logon and logoff event. Network monitor output showing the data transmitted between client and server. Event log data. Flat file showing the times recorded during execution of the cron job. Screen outputs showing successful bindings between clients and server. Test outputs include the verification (visual) that a file had been transferred to the DAAC. The successful completion of an E-mail message.

Success Criteria

This test will be deemed successful when all of the detailed functionality is verified.

Assumptions and Constraints

It is assumed that the DAAC file system will be populated with a number of directories, subdirectories, data files, and other objects. DAAC refers to the ECS deployed software. All workstations are configured to transfer and receive mail messages via E-mail. If an SCF is not available we will simulate the SCF functionality for IR-1. For IR-1, SCFs will have DCE clients at a minimum for the Primary Investigator. The PI will be responsible for distributing information among other scientists.

4.7.2 Test Case 2: Virtual Internetworking (BC023.002)

The purpose of the Virtual Internetworking test is to demonstrate the functionality of the integration of the Internetworking thread and GUI thread.

Test Inputs

Inputs to this test case include a series of Inter networking commands and commands to execute the GUI interface.

Test Steps

The test steps will be a regression of the tests from Sections 4.2 and 4.3 of this document

Test Outputs

Terminal sessions to emulated remote DAAC/SCF hosts. Demonstration of CSS common facilities and services. Logs and alarms showing recorded event data. The Directory/Naming Service should display all attribute types and attribute pairs for defined schema.

Success Criteria

This test will be deemed successful when users will be able to connect through remote virtual terminal sessions to DAAC and SCF hosts. This test will be deemed successful if all CSS Common Facilities and Services operate through GUIs.

Assumptions and Constraints

It is assumed that the file system will be populated with a number of directories, sub directories, data files, and other objects across the X/Open, X.500, and DNS name services.

4.7.3 Test Case 3: Messaging (BC023.003)

The purpose of the Messaging test is to demonstrate the functionality of the Message Passing Service. Distributed computing consists of several clients and server applications running on unique platforms. This interaction is classified in three categories: asynchronous, synchronous and deferred synchronous. The synchronous methods were tested within the IR-1 delivery and will be regression tested. Synchronous messaging occurs when a client makes a request and gives control to the server. In response the server services the request and returns the result to the client, at which point the client gets back control. Deferred synchronous mode occurs when the client makes a call and gets a ticket back from the server. The processing then takes place while the client and server are free to continue processing simultaneously. The results are then stored in an intermediate buffer where they can be retrieved at a later time by the client. Asynchronous mode occurs when the client makes a request without loosing control. The call will not return anything and is just used to pass data to a server. Client processing can continue simultaneously with the server processing. For example, FOS applications send real time data to SCF's asynchronously.

Test Inputs

Inputs to this test case include the transfer of some data between client and server and between server and client.

Test Steps

Develop a client/server application to pass a set of parameters between the client and the server

Initialize the server

Verify that the server is up and listening (waiting to be called by a client)

Run the client to pass a set of parameters back from the server

Verify that while the program is executing the client side is blocked until the server returns from the service

Verify that the set of numbers was passed between the client and server

Test drivers will be used to emulate an application with intense computations

Initialize the server to run in the background

Initialize the client

Verify that the client gets a ticket back from the server

Verify that while the computations are ongoing the client is still accessible

Verify that the client can later contact some intermediary, where the server has stored the results of the computation, to retrieve the results

Use a test driver to emulate an application which sends real time telemetry data to SCFs asynchronously

Initialize the server in the background

Initialize the client

Verify that while the data is being transferred to the server that the client can continue its processing

Verify that if the server is busy the data will be stored in an intermediary buffer

Verify that the sender can designate multiple receivers to receive the same message

Verify that multiple messages can be sent and that for each of these messages there is a different message queue to store the message

Send a message to the message queue

Set the time for the message to remain in the queue less than the time that the particular client checks its queue

Verify that when this time expires the message is deleted from the queue

Verify that a message is sent to the MSS management agent indicating that the time has expired and the message has been deleted

Verify that if a message can not be delivered and the time to delete the message has not yet expired, that the message is stored in the CSS message service

Verify that this message can be retrieved, whenever the receiver desires

Verify that the receiver checks the queue periodically not only when notified of a message

Verify that if there is not a message in the queue a null will be returned

Verify that when a receiver is not active the sender will periodically try to send the message to the receiver

Verify that the CSS message service provides an API for the receiver to register which sender they wish to receive messages

Test Outputs

Screen outputs showing that the server is up and running. Screen outputs showing that the client has been initialized. Screen outputs showing the results of the transaction. The client accessing of user survey questions. A history log indicating that the server was initialized and the client was started.

Success Criteria

This test will be deemed successful when all of the above functionality has been verified.

Assumptions and Constraints

To achieve asynchronous and deferred message passing, an intermediate buffering is maintained, which collects all the messages sent and then sends them to the intended receivers. Since the passing of the message from the sender to the message queue is synchronous, for every sender

there is a message queue on the same host. There are multiple instances of message queues so that processing is always continuing. Message queues support both push and pull models. Assumed that the service can locate and send messages to receivers.

4.7.4 Test Case 4: DOF Services (BC023.004)

The purpose of the DOF Services test is to demonstrate the functionality made available and support by the DOF Services.

Test Inputs

Inputs to this test case include: Interface Definition Language (IDL) and language mappings, software upgrading, calls between client and server, remote procedure calls, shutdown commands, unretrievable binding information and communications between the TCP and UDP protocols.

Test Steps

Verify that the DOF provides an IDL and language mappings to C and C++.

Verify that the IDL supports minor and major versioning, minor versions should be upward compatible requiring no changes in the client software to communicate with the new implementations.

Generate an error in the calls between the client and server, verify that the general error status is passed as a parameter.

Verify that the DOF can marshal and unmarshal the arguments transparently while making an rpc or standard types to/from a common standard format or routines for user defined types.

Shutdown a service, verify that the DOF provides a mechanism to gracefully shutdown the service, by allowing the servers to unregister the server information from the namespace.

Verify that when a binding can not be resolved or a binding service can not be retrieved, the DOF returns an exception or error gracefully.

Verify that the TCP and UDP protocols are supported by the DOF.

Test Outputs

Outputs to this test case include: IDL and language mappings to C and C++, new versions with little changes required to the client software, an error status passed as a parameter, marshalled and unmarshalled arguments, unregistered server information from the namespace and an error for an unretrievable binding.

Success Criteria

This test will be deemed successful when all of the above functionality is verified through inspection, demonstration or test.

Assumptions and Constraints

None.

4.7.5 Test Case 5: DOF API (BC023.005)

The purpose of the DOF API test is to demonstrate the functionality made available and supported by the CSS provided DOF APIs.

Test Inputs

Inputs to this test case include API calls to: register/unregister services in the namespace, register/unregister interfaces, register services using different protocols, limit the maximum number of threads to use in servicing the requests concurrently, bind to services, set/get the authentication and authorization used between clients and servers, maintain the integrity and privacy of the data passed between client and server and set the identity of a given principal to a given process.

Test Steps

Run an XRunner script to call the various DOF APIs.

Test Outputs

Outputs to this test case include responses to all of the API calls.

Success Criteria

This test case will be successful when all of the API calls perform the appropriate functionality.

Assumptions and Constraints

None.

4.7.6 Test Case 6: Time Services (BC023.006)

The purpose of the Time Services test is to demonstrate the functionality made available and supported by the Time Services API.

Test Inputs

Inputs to this test case include a group of API calls demonstrating the timestamping and converting functionality provided by the CSS Time Service.

Test Steps

Use XRunner to make a variety of API calls.

Verify that an API to retrieve timestamp information is provided.

Test the API to verify its ability to convert between binary timestamps that use different time structures.

Verify that a provided API will convert between binary timestamps and ASCII representations, between UTC time and local, and between binary timestamps that use different time structures.

Verify that the provided API can manipulate binary timestamps.

Verify that the CSS Time Service provides APIs to compare two binary time values, calculating binary time values, and obtaining time zone information.

Test Outputs

Outputs to this test case include a variety of API calls resulting in the converting, manipulating and retrieving various formats of time stamps.

Success Criteria

This test will be deemed successful when all of the functionality provided with the CSS Time Service API has been tested and verified.

Assumptions and Constraints

None.

4.7.7 Test Case 7: CSS Interfaces (BC023.007)

The purpose of the CSS Interfaces test is to demonstrate the interfaces that exist between CSS and SDPS, CSS and FOS, and CSS and ISS. The SDPS and FOS interfaces will be simulated in the testing facility.

Test Inputs

Inputs to this test case include: an event, a message, electronic mail, bulletin board, a service request, lower layer ISO services (TCP/UDP/IP), etc.

Test Steps

Simulate the SDPS interface.

Verify that the CSS API can send data, as defined in Table 6-1 of the Communications and System Management Segment (CSMS) Requirements Specification for the ECS Project (304-CD-003-002), to the SDPS subsystem (simulated).

Verify that the CSS server can send data, as defined in Table 6-1 of the Communications and System Management Segment (CSMS) Requirements Specification for the ECS Project (304-CD-003-002), to the SDPS subsystem (simulated).

Verify that the CSS server can receive a service request and authenticate V0 clients to ECS for any SDPS subsystem (simulated).

Simulate the FOS interface.

Verify that the CSS API can send data, as defined in Table 6-1 of the Communications and System Management Segment (CSMS) Requirements Specification for the ECS Project (304-CD-003-002), to the FOS subsystem (simulated).

Verify that the CSS server can send data, as defined in Table 6-1 of the Communications and System Management Segment (CSMS) Requirements Specification for the ECS Project (304-CD-003-002), to the FOS subsystem (simulated).

Verify that the CSS server can receive a service request and authenticate V0 clients to ECS for any SDPS subsystem (simulated).

Verify that the CSS can send information to the ISS lower level ISO services, as defined in Table 6-4 of the Communications and System Management Segment (CSMS) Requirements Specification for the ECS Project (304-CD-003-002).

Test Outputs

Outputs to this test case include, but are not limited to, the successful communications between CSS and ISS, CSS and FOS, and CSS and SDPS.

Success Criteria

This test will be deemed successful when all of the data defined has been communicated over the provided interface(s) [SDPS and FOS interfaces will be simulated].

Assumptions and Constraints

The simulated SDPS and FOS interfaces will be functionally identical to the actual interfaces. The ISS communications layers have already been set in place.

4.8 Security Management Thread Test (TC024)

This thread verifies the functionality of Security Management Service. This service includes secure user logon/logoff, maintenance of the user authentication directory, use and maintenance of access control lists, network and system security management and security compliance management. Baseline technologies for these services include DCE and HP OpenView.

The objective of this thread is to verify that appropriate Release A security can be achieved and maintained.

Special resources required for this thread test include:

- XRunner
- HP OpenView
- Network analyzer
- Isolated processor for virus detection testing
- Randomly selected set of viruses
- Security Registry and ACL file maintenance programs
- Network device, processor, and application management agents
- Security Compliance Test Suites

This thread contains 14 test cases:

4.8.1 Test Case 1: Authentication Regression Testing (TC024.001)

This test case regression tests IR-1 authentication capability. Regression testing will include:

1. Logon/Logoff
2. Failed logon
3. Password Change
4. Password Reset
5. Security Registry Maintenance
6. Security Privilege Test

Description of this testing is contained in Section 4.3 of Volume 1 of the CSMS I&T Plan.

4.8.2 Test Case 2: Process to Process Authentication (TC024.002)

This test case verifies authentication for process to process actions.

Test Inputs

Security registry entries that establish a set of process to process privilege. A set of test drivers that generate process to process actions.

Test Steps

Run test drives to invoke both valid and invalid process to process actions.

Logon using a valid user ID and password.

Using a network analyzer, verify that the password is encrypted as it passes from the security registry to the client.

Test Outputs

System management logs showing failed invalid process to process actions. Network monitor output showing the data transmitted between the client and server.

Success Criteria

Non-authenticated actions as defined by the Security Registry failed and logged (alarmed if appropriate) and authenticated actions allowed. The Data Encryption Standard (DES) for encryption and decryption of data is supported.

Assumptions and Constraints

None

4.8.3 Test Case 3: Authentication Expiration (TC024.003)

This test case verifies that authentication tickets granted to users and processes expire in the configured time.

Test Inputs

A registry data base with a test set of process and user privileges.

A set of valid user ID and passwords.

Test drivers providing process to process actions.

Test Steps

Set ticket expiration time parameter to a short period of time.

Log users on and exercise valid user system privileges.

Run process test drivers exercising valid system privileges.

Wait till ticket expiration time expires.

Repeat user and process privilege actions.

Modify ticket expiration time and repeat the test steps.

Test Outputs

System logs showing failed privilege attempts.

Success Criteria

Privilege allowed prior to ticket expiration. Privilege disallowed after ticket expiration.

Assumptions and Constraints

None.

4.8.4 Test Case 4: Access Control List Maintenance (TC024.004)

This test case verifies the ability to create and maintain Access Control Lists (ACL).

Test Inputs

Valid ACL administrator ID and password.

Non ACL administrator ID and password.

A set of ACL add, change, and delete transactions.

Test Steps

Logon with valid ACL administrator ID and password.

Perform add, change, and delete transactions on ACL files.

Logon with a non ACL administrator ID and password.

Perform add, change, and delete transactions on ACL files.

Save the ACL database using the CSS provided API.

List the resulting ACL files.

List any error reports

Test Outputs

Screen outputs showing the success or failure of the maintenance transactions. A listing of the resulting ACLs after maintenance.

Success Criteria

Valid maintenance transaction processed successfully. Invalid transactions shown on error lists. ACL files correctly reflect the results of the correct maintenance transactions. All non administrator transactions fail.

Assumptions and Constraints

None.

4.8.5 Test Case 5: Access Control List Security (TC024.005)

This test case verifies ACL security is maintained.

Test Inputs

User and process actions that perform valid and non valid file access attempts.

Test Steps

Logon with valid user ID and password combinations representing varied user privilege.

Attempt to access files that the IDs are privileged to access.

Attempt to access files that the IDs are not privileged to access.

Run processes that attempt both valid and invalid file accesses.

Test Outputs

System logs showing the success or failure of the of the use of file access privilege.

Success Criteria

Valid privilege use allowed, Invalid privilege use disallowed. System log records showing invalid attempts.

Assumptions and Constraints

None.

4.8.6 Test Case 6: Site System and Network Security Management (TC024.006)

This test case verifies the site system and network security management capabilities for Release A.

Test Inputs

User and process actions that perform valid privilege and non valid privilege actions, for example file and data base access. User valid and invalid logons. Anomalous network traffic that simulates intrusion or denial of access attacks. Site Security management log analysis programs. Security tests. Security audit trails.

Test Steps

Run multiple test scripts that use the above described inputs to create security management events. Run security management log analysis programs. Run security tests for password auditing, file system integrity checking, auditing of user privileges and auditing of resource access control information. Security tests should be performed on a periodic and interactive basis. Transfer the results of the tests to the EMC. Designate a user, group of users or M&O staff to receive notification upon detection of an intrusion. Verify that the appropriate users and/or M&O staff were notified of the detection. Analyze the security audit trails to detect login failures, unauthorized access to resources and break-ins. Verify that the notification was received within 5 minutes. Corrupt some of the data, verify that the compromised area is isolated until the compromise has been eliminated.

Test Outputs

System Management logs. Security Management alarms in HP OpenView. Listing of log data prepared for upload to the SMC. Results of the security tests. Notifications to appropriate users and M&O staff. An isolated area of data containing the corrupted data.

Success Criteria

Security events correctly logged and alarmed where appropriate. No logging or alarming of non valid security events (some security events will appear as fault or performance problems, these will be considered valid). Successful analysis of systems logs to identify security violation patterns and the generation of appropriate alarms within 5 minutes of analysis of the logs. The appropriate data for upload to the SMC is prepared.

Assumptions and Constraints:

Log data is analyzed on a consistent basis to identify potential security events.

4.8.7 Test Case 7: Virus Detection (TC024.007)

This test case verifies Security Management Services ability to detect and eradicate viruses.

Test Inputs

A randomly selected set of known viruses.

Test Steps

On an isolated processor introduce viruses into the system. Have the virus detection software enabled. For identified viruses run the virus eradication software. Run a follow-up (possibly different virus detection program).

Test Outputs

System logs indicating detected viruses. Operator displays indicating detected viruses. Virus eradication software reports. Follow-up virus detection report output.

Detection and identification of introduced viruses. Eradication software reports showing successful eradication of viruses. A clean follow-up virus scan.

Assumptions and Constraints

None.

4.8.8 Test Case 8: SMC System and Network Security Monitoring (TC024.008)

This test case verifies SMC System and Network Security Monitoring

Test Inputs

Simulated log inputs from multiple DAACs including security event data that taken in aggregate shows patterns of intrusion.

Test Steps

Run SMC log analysis programs against the simulated DAAC log data..

Test Outputs

Log analysis reports and system management alarms.

Success Criteria

Appropriate identification of potential security intrusion.

Assumptions and Constraints

DAAC refers to the ECS deployed software.

4.8.9 Test Case 9: Security Management Compliance (TC024.009)

This test case verifies security compliance audit capabilities.

Test Inputs

Security compliance test suite.

Test Steps

Configure an emulated DAAC environment with security management capabilities in place.

Introduce non compliance cases, for example non compliant passwords.

Run security compliance test suite both an LSM and SMC version. .

Test Outputs

Compliance test suite analysis reports.

Success Criteria

Identification of non compliance items.

Assumptions and Constraints

DAAC refers to the ECS deployed software.

4.8.10 Test Case 10: Security Database (TC024.010)

This test case verifies security database compliance.

Test Inputs

Typical DAAC system management logs including security events.

Test Steps

Run log analysis and database upload processes against logs.

Test Outputs

Reports from both the SMC and LSM databases.

Success Criteria

Log data correctly recorded in both LSM and SMC databases.

Assumptions and Constraints

DAAC refers to the ECS deployed software.

4.8.11 Test Case 11: Security Reporting (TC024.011)

This test case verifies security data base compliance.

Test Inputs

A populated system management database including security data.

Test Steps

Run security reporting suite against database.

Run ad hoc reports against database.

Using the SMAS Run reports for the collected management data, such as login failures, unauthorized access to ECS resources and break-ins.

Verify that these reports can be redirected to the console, a disk file and a printer.

Test Outputs

Reports from both the SMC and LSM databases.

Success Criteria

Required reports correctly produced from data base. Correct reports based on the input ad hoc criteria.

Assumptions and Constraints

None.

4.8.12 Test Case 12: Security Recovery (TC024.012)

This test case verifies security recovery compliance.

Test Inputs

Security recovery procedures.

Test Steps

Inspect security recovery procedures for the LSM and SMC for compliance with recovery requirements.

Test Outputs

Inspection of the evaluated reports

Success Criteria

Compliance with requirements.

Assumptions and Constraints

None.

4.8.13 Test Case 13: Security Policies and Procedures (TC024.013)

This test case verifies security policy and procedure compliance.

Test Inputs

Office automation tools to be used for policy and procedure management and flowdown.

Test Steps

Inspect office automation tools to determine capability to meet policy and procedure management and flowdown requirements.

Test Output

Inspection of the evaluated reports

Success Criteria

Compliance with requirements.

Assumptions and Constraints

None.

4.8.14 Test Case 14: EMC Security Management (TC024.014)

This test case verifies the EMC Security Management capabilities for Release A.

Test Inputs

Suite of security tests, results of the tests, notification of security events, security audit trail from the sites, recovery procedures and recovery procedures from a detection.

Test Steps

From the EMC request a security test for the sites (on a scheduled and interactive basis). Verify that at the EMC you can support, manage and maintain this test. Retrieve the results of the tests from each of the sites. Verify that when a security event occurs at a site the site Security Management Application notifies the EMC Security Management Application. Verify that the EMC receives the security audit trails from the sites and analyzes the audit trails to detect intrusions. Verify that the EMC coordinates and sends the recovery procedures to the sites.

Test Outputs

Outputs include: security tests executed at the sites, results of the tests sent to the EMC, notification of the EMC from the site when the detection occurs, receipt of the security audit trails from each of the sites, a report showing the analyzes of the audit and recovery procedures.

Success Criteria

This test will be deemed successful when security tests are executed for each of the sites, results of the tests forwarded to the EMC, detection of intrusion and notification of the EMC and recovery procedures distributed from the EMC to the sites.

Assumptions and Constraints

None

4.9 Network Security Thread Test (TC025)

This thread demonstrates the functionality of network security for Release A. This test will be limited to network device security functions. Network security management functions will be tested as part of the Security Management Thread.

The objective of this thread is to prove that network devices are providing the required security services and security notifications to the Site Security Management Application Service.

Special resources required for this thread test include:

- HP OpenView
- Network analyzer
- Network traffic generator
- Network device configuration interfaces

This thread contains 2 test cases:

4.9.1 Test Case 1: Network Filtering Test (TC025.001)

This test demonstrates the network device filtering of packets on port/socket and/or source and/or destination address.

Test Inputs

Router configurations establishing filtering conditions. Test packets with combinations of port/socket identification and source/destination addresses.

Test Steps

Run telnet, remote log on, file transfer, and interprocess jobs that create the above described test packets.

Test Outputs

Network management logs showing the success or failure to the various packets in getting through the network device filters.

Success Criteria

Not allowed packets fail, allowed packets passed. Log records of failed packets. Security alarms to Site Security Management Services if appropriate.

Assumptions and Constraints

This functionality will be further verified implicitly in other build/thread tests since Inter networking will be a part of most other tests.

4.9.2 Test Case 2: Network Device Intrusion Detection (TC025.002)

This test demonstrates the network device's ability to identify anomalous data traffic that may be an indication of a security intrusion.

Test Inputs

Network load from network traffic generator.

Test Steps

Run network traffic generator to simulate possible network intrusion or denial of service activities. Run network traffic generator to simulate normal network traffic.

Test Outputs

Network management logs showing the detection of anomalous network events and appropriate alarms to Site Security Management Services.

Success Criteria

Correct identifications of network anomalies and no anomaly logging during normal traffic conditions.

Assumptions and Constraints

Network devices will identify security intrusions as performance or fault conditions. Site security Services or the Enterprise Monitoring Center will provide the analysis to determine if there is a potential security intrusion. This functionality will be further verified implicitly in other build/thread tests since Inter networking will be a part of most other tests.

4.10 System Security Build Test (BC026)

The System Security Build test represents the integration of the CSS and ISS functionality for Release A. This test is an aggregation of the Communications Services Build and Security Management and Network Security threads. The functionality regression tested from IR-1 include: file transfers, communication via the internet, demonstrate ACLs and communications with external interfaces. Release A functionality tested includes: multicasting, file access virtual terminal, DCE enhancements, network security and security management.

The objective of this test is to verify that all of the previously tested functionality is still available upon integration of the System Security Build.

Special resources required for this thread test include:

- Sensor Data Processing Facility (SDPF) simulator
- TRMM Science Data and Information System (TSDIS) simulator
- NOLAN emulation, for example protocols
- Emulated IR-1 DAAC configuration
- HP OpenView
- Network analyzer
- NSI and ESN V0 connections
- XRunner
- Hardware vendor diagnostics

This thread contains 2 test cases.

4.10.1 Test Case 1: Communication Services Integration (BC026.001)

The purpose of the Communication Services Integration test is to verify that the functionality available in the Communication Services Build is functional upon integration with the Security Management and Network Security threads. To verify the Release A CSS and ISS requirements are met.

This test case regression tests the Communication Services Build (previously tested in Section 4.7) with the integration of the Security Management and Network Security threads.

4.10.2 Test Case 2: Release A Integration (BC026.002)

The purpose of the Release A Integration test case is to test the Security Management and Network Security Threads upon integration with the Communication Services Build.

Test Inputs

Inputs to this test case include: logon attempts with valid/invalid user name/password combinations, password change, password reset, security registry entrants, drivers to generate process to process actions, DCE administrator privileges, rgy_edit commands, network traffic to simulate intrusion or denial of access attacks, log inputs from the DAACs, viruses, populated system management database, recovery procedures, routing configurations, test packets and simulated network load.

Test Steps

Attempt to logon using combinations of valid/invalid user names and passwords

Change a user's password

Reset a user's password

Initialize drivers to invoke both valid and invalid process to process actions

Upon successful login, verify that you have been granted a ticket

Set the ticket expiration time for a shorter duration

Logout and log back in

Verify that you can execute your binding call

Once ticket time expires, verify that you can not execute your binding call

Login as a valid DCE administrator

Perform add, change and delete transactions on ACL files

Verify that the ACL has been updated

Verify that the ACL users are only able to execute the privileges they have been granted

Create security management events

Verify that the events have been captured

Run the security management log analysis program

Introduce a virus (on an isolated processor)

Verify that the virus detection software detects the virus

Run security compliance test reports for both LSM and SMC and verify that the reports are consistent

Run all appropriate reports and detection tools

Run the network traffic generator to load the network

Verify that the system can detect the increased volume

Test Outputs

Test outputs include: systems management logs showing failed invalid process to process actions, a variety of system logs, screen outputs showing the success or failure of the maintenance transactions. Listings of ACLs indicating changes, alarms in notification in OpenView, operator displays indicating detected viruses, reports from both SMC and LSM, and network logs showing the success of the packets to get to their destination and detection of anomalous network events.

Success Criteria

This test will be deemed successful when: non authenticated actions fail and get logged and authenticated actions are allowed, allowed privileges prior to ticket expiration and disallowed privileges upon ticket expiration, valid maintenance transaction processed successfully, documented invalid transactions, valid ACL privileges allowed and invalid privileges disallowed, detection and identification of viruses, identification of non compliance items, correctly logged data at both the LSM and SMC, correct identification of network anomalies and in all cases compliance with the requirements.

Assumptions and Constraints

Log data is analyzed periodically to identify potential security events. The functionality will be further verified implicitly in other build/thread tests since Inter networking will be a part of most other tests.

4.11 Systems Logistics Management Thread Test (TC027)

The purpose of this thread is to verify the functionality of the Systems Logistics Management Service, which performs baseline management, software change management, and change request management services. This thread includes the regression testing (IR-1 functionality) of those Configuration Management Application Service (CMAS) functions dealing with maintaining configurable items (except hardware), managing software changes, and performing automated

builds. ClearCase is the chosen CM tool for Release A, and Distributed Defect Tracking System (DDTS) is the chosen Change Request Manager tool.

Special resources required for this thread test include:

- Clearcase (with various privileges, triggers and notification scripts)
- DDTS
- Baseline Manager custom code

This thread contains 7 test cases.

4.11.1 Test Case 1: Configuration Management Regression Testing (TC027.001)

This test case regression tests the IR-1 Configuration Management capabilities. Regression testing will include:

1. Maintenance of Configurable Items
2. Software Change Management
3. Build Process Audit

A description of this testing is contained in Section 4.15 of Volume 1 of the CSMS I&T Plan.

4.11.2 Test Case 2: Maintenance of Configured Hardware (TC027.002)

This test case will demonstrate the ability to access and display vital information for each of the unique hardware items under configuration control.

Test Inputs

Inputs to this test case include Baseline Manager custom code commands.

Test Steps

Log onto a DAAC workstation.

Access and display the names and unique identifiers for each ECS hardware CI and its components deployed to the local site.

Access and display the historical status (versions, baselines, level of assembly, history of changes, release configuration, etc.) for a sample of the configured hardware.

Access and display a sample of the related hardware specification, technical, operations, and maintenance documentation.

Access and display the current hardware configuration resident at the local site.

Repeat the above steps for a configuration software item.

Test Outputs

The expected results of this test include the ability to access all requested hardware and software information.

Success Criteria

This test will be deemed successful when all of the commands return the desired results.

Assumptions and Constraints

It is assumed that the DAAC file system will be populated with a number of hardware items to be managed by CMAS.

4.11.3 Test Case 3: Change Request Management (TC027.003)

This test case will demonstrate the ability of the CMAS to register non-conformance reports and configuration change requests electronically.

Test Inputs

Inputs to this test case include DDTS commands.

Test Steps

Log onto a DAAC workstation.

Activate the DDTS tool.

Compose a request for system changes by responding to prompts for relevant information.

After committing the change request information, verify that an identifier has been assigned to the request. (Repeat for ECS system change, verifying that the capability with which to compose ECS requests for systems changes is provided.)

Forward the request to the EMC.

Verify that the request has been received by the SMC.

Ensure that the request has been distributed to the appropriate organizations for consideration.

Submit an impact response to the change request, and verify that the SMC received and stored the impact assessment, verify that this information is available system-wide.

Verify that the impact assessment has been electronically linked to the request.

Check the status of an existing impact response to change evaluation requests and verify that the information is maintained in the SMC, verify that this information is made available system-wide.

Verify that the change requests, assessments, and status is made available for system-wide viewing.

Verify that the SMC maintains a historical record of ECS system impact assessments, this should contain proposed and approved requests, track the approval of status of proposed changes and system-wide lists of the identity and disposition of changes proposed to the ECS.

Test Outputs

The expected results of this test include a newly generated change request which has been distributed as assigned and maintains a current approval status.

Success Criteria

This test will be deemed successful when a user is able to electronically draft a change request, mail it, and track it through the approval process.

Assumptions and Constraints

None

4.11.4 Test Case 4: SMC CM (TC027.004)

This test case will demonstrate the functionality of CMAS at the SMC.

Test Inputs

Inputs to this test case include: SCF-provided configuration data for individual algorithms, ECS configuration controlled items, ECS documents, ECS-developed resources, ECS releases, Software-critical and security-sensitive items lists, scientific algorithms and ECS files, change requests via electronic mail, and impact assessment and change evaluation requests.

Test Steps

Enter an algorithm into the CMAS

Verify that the algorithm information includes the SCF provided data (algorithm development version numbers, identification codes, reference numbers, SCF point of contact's name and organization, associated file names, formats, sizes and descriptions, number of files by category and type).

Enter a configuration controlled item into the CMAS

Verify that the SMC makes available system-wide a name and unique identifier for the entered ECS configuration-controlled items including all of the appropriate ECS information

Verify that the ECS controlled items are characterized as either system-wide or site-specific

Verify that information containing the sites where individual versions of controlled items are located and the operational status of that version at the site are obtainable

Update a previous ECS hardware or software resource (thus updating the version number)

Verify that SMC maintains records that identify the current and previous versions (ECS hardware and software resources and documents) and makes this information available system wide

Update a software item, changing the version number of the release at each site (repeat for a hardware item).

Verify that the SMC retains records of this baseline change and distributes the records to each site.

Verify that the SMC retains reports indicating specifications and technical, operations, and maintenance documentation, and the identity and change status of documents associated with each version of ECS hardware and software resources deployed and distributes it to each site

Deliver a new version of software to the sites, verifying that the SMC maintains and distributes to the sites a report which describes the change requests satisfied by the new versions (repeat this step for new hardware and documentation releases).

Verify that historical status records (latest baseline and changes, baseline history, latest release documentation, etc.) can be easily retrieved from the SMC.

Update a software release that only affects a limited number of sites.

Verify that historical status records of ECS baseline changes to sites affected, and installation schedule and installation status are easily retrievable from the SMC.

Verify that the SMC maintains a software-critical and security-sensitive items list.

Verify that the identity and change status of individual ECS resources deployed to the sites is reported by the SMC.

Verify that the SMC shall assemble unlicensed toolkit software files to be posted to the bulletin board. These files should consist of source code, linkable object code, make files, and installation procedures.

Test Output

Outputs to this test case include: reports documenting individual versions of CIs location and operational status, records maintaining software and hardware change items, baseline changes, maintenance documentation, identity and change status of documents associated with each version, change requests satisfied by each release, historical status records, name and unique identifiers for the entered ECS CIs and a posted toolkit software file.

Success Criteria

This test will be deemed successful when all of the documented test steps have been successfully completed.

Assumptions and Constraints

None.

4.11.5 Test Case 5: CMAS SMC Functionality (TC027.007)

This test case will demonstrate additional CMAS functionality available at the SMC.

Test Inputs

Inputs to this test case include: SCF-provided configuration data for individual algorithms, ECS configuration controlled items, ECS documents, ECS-developed resources, ECS releases, Software-critical and security-sensitive items lists, scientific algorithms and ECS files, change requests via electronic mail, and impact assessment and change evaluation requests.

Test Steps

Demonstrate that the CMAS tracks the names and identifiers for the following items deployed at the sites: ECS subsystems, networks, and configured system and network devices such as workstations, servers, and routers; ECS releases and baselines; ECS hardware and software resources designated as configuration items; technical documentation and test materials; scientific algorithms, including software, data and test materials (DAAC's only); algorithm processing logic control and calibration coefficients data; algorithm test documentation, including specifications, data files, scripts.

Verify that the SMC CMAS maintains and makes available system wide, all sites where individual versions of CIs are located and the operational status of that version at the site.

Demonstrate the ability of the CMAS to make available system-wide, records that identify the current and previous versions of ECS hardware and software resources deployed to the sites.

Verify that the CMAS at the SMC shall maintain records that identify the current and previous versions of documents associated with the deployed ECS resources.

Demonstrate the ability of the CMAS at the SMC to distribute to each site records that identify the baseline changes included in each release of ECS hardware and software deployed at the site.

Demonstrate the ability to distribute to each site, record that identify the specifications and technical, operations, and maintenance documents associated with versions of ECS hardware and software configuration items deployed to the site.

Verify that the CMAS at the SMC distributes records to each of the sites that describes any changes to the baselines.

Verify that the CMAS at the SMC maintains historical records about ECS CIs system wide that include: current version; current version's specifications and technical, operations, and maintenance documentation; specifications and technical documentation history; "level of assembley" representation of components comprising the item's courrent release configurations; and version history.

Verify that the CMAS at the SMC maintains historical records about ECS system releases that include: latest baseline plus approved changes; baseline history; latest release documentation; "level of assembly" representation of the subsystem and configuration item versions that comprise the release configuration; history of changes, including changes to subordinate units/components; effectivity and installation status at operational sites; and release configuration.

Verify that the CMAS at the SMC maintains historical records about ECS baseline changes that include: sites affected; installation dates; and installation status.

Verify that software-critical and security-sensitive items lists are maintained by the SMC CMAS.

Verify that the service makes available system-wide, reports that contained the identity and change status of individual ECS resources deployed to the sites and reports containing the identity of resources comprising ECS baselines and releases.

Test Outputs

Outputs to this test case include: the demonstration that a variety of records are maintained by the CMAS and that the information mentioned above is available in these references.

Success Criteria

This tes case will be deemed successful when all of the information above is demonstrated in the appropriate record maintained by the CMAS at the SMC.

Assumptions and Constraints

None.

4.11.6 Test Case 6: EMC CM (TC027.005)

This test case will demonstrate the functionality of CMAS at the EMC.

Test Inputs

Inputs to this test case include: SCF-provided configuration data for individual algorithms, ECS configuration controlled items, ECS documents, ECS-developed resource, ECS releases, Software-critical and security-sensitive items lists, scientific algorithms and ECS files, change requests via electronic mail, and impact assessment and change evaluation requests.

Test Steps

Log onto the CMAS at each site.

Verify that when a new baseline is configured at one of the sites, the site CMAS identifies the new baseline and reports the information to the EMC.

Verify "level of assembly" descriptions of operational baselines at the sites are made available to the EMC.

Verify that each site maintains information identifying versions and implementation status of configuration-controlled items at the sites and makes this information available to the EMC.

Verify that, at each site, the CMAS maintains historical status records (including current version, documentation history, etc.) for ECS and algorithm software at the site.

Verify that the CMAS at the EMC and individual sites shall maintain records to establish traceability among operation baselines and releases, and maintain "level of assembly" descriptions of controlled item components.

Test Outputs

A successful logon to the local CMAS at each site. An output indicating the characteristics of the resources at each site. Messages sent to the EMC by the site CMAS indicating: a new baseline at one of the sites, descriptions of what makes up the baselines, and version and implementation information. Historical status records, traceability records and algorithms and SDPS data files ingest to the subsystem.

Success Criteria

This test case will be deemed successful when all of the functionality associated with the local CMAS has been demonstrated/tested and verified.

Assumptions and Constraints

Software versions have already been loaded into the CM tool at the individual DAACs.

4.11.7 Test Case 7: General CM (TC027.006)

This test case will demonstrate the functionality of CMAS.

Test Inputs

Inputs to this test case include: SCF-provided configuration data for individual algorithms, ECS configuration controlled items, ECS documents, ECS-developed resources, ECS releases, Software-critical and security-sensitive items lists, scientific algorithms and ECS files, change requests via electronic mail, and impact assessment and change evaluation requests.

Test Steps

Verify that a user can checkout from CM the algorithms and associated data files for construction of builds.

Verify that a user can checkin the algorithms and associated data files for construction of builds that are stored in the CM tool.

Verify that there is a site software library under CM control.

Verify that all ECS-controlled resources are characterised as system-wide or site specific.

Bring up a software version at one of the DAACs, verifying that the CMAS identifies status for each version of every site-controlled item, reflecting the lifecycle stage to which it has been promoted.

Verify that the CMAS produces formatted data files containing baseline management data records.

Verify that the CMAS accepts and stores baseline management data records provided by formatted data files and the interactive user interface.

Verify that for each event that operation type, user id of initiator, date-time stamp and host name are logged.

Demonstrate the capability of the M&O staff to generate reports for time frames, operation types, user IDs and hosts.

Test Outputs

Checked out and checked in algorithms and data files, inspected site software library, inspected software version, formatted data files, and generated reports.

Success Criteria

This test case will be deemed successful when all of the outlined functionality has been demonstrated and verified.

Assumptions and Constraints

This test case will cover all CM related requirements which do not fit to a specific test case or any new requirements which may be derived.

4.12 Performance Management Thread Test (TC028)

The purpose of this thread is to verify the Release A functionality of the Performance Management Application Service. This thread will test the ability of the MSS Performance Management Application Service to provide performance data monitoring, trending, testing, and reporting. HP OpenView Network Node Manager is the chosen performance management tool for Release A.

Special resources required for this thread test include:

- Operational DCE cell
- XRunner
- LoadRunner
- HP OpenView Network Node Manager
- Network components (routers, links, bridges, and gateways)
- Hosts (operating systems, peripherals, and databases)
- Operational performance benchmark test procedure suite

This thread contains 10 test cases.

4.12.1 Test Case 1: Alarm Processing and Display Regression Testing (TC028.009)

This test case regression tests IR-1 Alarm Processing and Display capabilities. Regression testing will include:

1. Basic Monitoring
2. OpenView
3. Fault Indication

A description of this testing is contained in Section 4.14 of Volume 1 of the CSMS I&T Plan.

4.12.2 Test Case 2: Performance Monitoring of Network Components (TC028.001)

This test case will demonstrate the ability to monitor, display, and print the performance parameters of external and internal (site) network components on demand and at configured intervals.

Test Inputs

Inputs to this test case include HP OpenView Network Node Manager commands, XRunner scripts, and LoadRunner scripts.

Test Steps

For specified local and external network routers, request (on demand), display, and print the following:

- operational status (on-line, off-line, or test mode)
- type
- speed
- octets in/out
- packets in/out
- discards in/out
- errors in/out

Repeat above for specified local and external network links.

Repeat above for specified local and external network bridges.

Repeat above for specified local and external network gateways.

Utilize various configurable intervals for automatic performance monitoring, noting the above performance parameters for the aforementioned network components.

Via LoadRunner, determine the number of network components which can be monitored without loading down the system excessively.

Test Outputs

The expected results of this test include the ability to accurately and promptly report performance information for monitored network components.

Success Criteria

This test will be deemed successful when all of the designated network components report the requested performance information in a timely manner.

Assumptions and Constraints

It is assumed that normal network traffic will be present during testing.

4.12.3 Test Case 3: Performance Monitoring of Hosts (TC028.002)

This test case will demonstrate the ability to monitor, display, and print the performance parameters of hosts on demand and at configured intervals.

Test Inputs

Inputs to this test case include HP OpenView Network Node Manager commands, XRunner scripts, and LoadRunner scripts.

Test Steps

For specified operating systems, request (on demand), display, and print the following:

- total CPU utilization
- memory utilization
- physical disk I/Os
- disk storage size
- disk storage used
- number of active processes
- length of run queue
- network I/0s (packets)
- network errors

Repeat above for specified local and external peripherals, also noting operational status (on-line, off-line, or test mode).

Repeat above for specified local and external databases.

Utilize various configurable intervals for automatic performance monitoring, noting the above performance parameters for the aforementioned hosts.

Via LoadRunner, determine the number of hosts which can be monitored without loading down the system excessively.

Test Outputs

The expected results of this test include the ability to accurately and promptly report performance information for monitored hosts.

Success Criteria

This test will be deemed successful when all of the designated hosts report the requested performance information in a timely manner.

Assumptions and Constraints

It is assumed that a number of hosts will be available for monitoring.

4.12.4 Test Case 4: Performance Monitoring of Communication Protocol Stacks (TC028.003)

This test case will demonstrate the ability to monitor, display, and print the performance parameters of communication protocol stacks on demand and at configured intervals.

Test Inputs

Inputs to this test case include HP OpenView Network Node Manager commands, XRunner scripts, and LoadRunner scripts.

Test Steps

For specified communication protocol stacks on internal (site) managed devices, request (on demand), display, and print the following:

- number of transport layer messages received with errors
- number of transport layer messages requiring re transmission
- number of transport layer messages received that could not be delivered
- number of network layer messages received with errors
- number of network layer messages received that could not be delivered
- number of network layer messages that were discarded

Repeat above for specified communication protocol stacks on external devices.

Utilize various configurable intervals for automatic performance monitoring, noting the above performance parameters for the aforementioned communication protocol stacks.

Via LoadRunner, determine the number of communication protocol stacks which can be monitored without loading down the system excessively.

Test Outputs

The expected results of this test include the ability to accurately and promptly report performance information for communication protocol stacks on managed devices.

Success Criteria

This test will be deemed successful when all of the designated communication protocol stacks report the requested performance information in a timely manner.

Assumptions and Constraints

It is assumed that a number of communication protocol stacks will be available for monitoring.

4.12.5 Test Case 5: Performance Monitoring Thresholds (TC028.004)

This test case will demonstrate the ability of the MSS Performance Management Application Service to provide a number of configurable thresholds for each performance metric, provide default values, allow for the modification of these values, and compare received values against these thresholds.

Test Inputs

Inputs to this test case include HP OpenView Network Node Manager commands and ECS performance data. A list of initial thresholds.

Test Steps

Examine a listing of all MSS Performance Management Application Service thresholds to ensure that a configurable value exists for all measured performance data listed in TC025.001 through TC025.003.

Verify that you can send a list of suggested initial thresholds for each performance metric to the MSS site performance management application via CSS services and that the sites can receive it.

Examine the above list to ensure that a suggested initial threshold value exists for each performance metric.

Re configure several of these threshold values to higher settings.

Re configure several of these threshold values to lower settings.

Rerun several steps from TC028.001 through TC028.004, ensuring that several monitored parameters will surpass those thresholds set to lower values.

Ensure that the proper alarms/warning have been disseminated concerning any values exceeding their thresholds.

Test Outputs

The expected results of this test include the ability to accurately compare received performance metrics to configured thresholds. A list of initial thresholds at the sites.

Success Criteria

This test will be deemed successful when all performance parameters exceeding their configured thresholds are flagged.

Assumptions and Constraints

It is assumed that TC028.001 through TC028.004 have been successfully completed.

4.12.6 Test Case 6: History Log Verification (TC028.005)

This test case will demonstrate the ability of the MSS Performance Management Application Service to log all ECS performance data in the History Log.

Test Inputs

Inputs to this test case include HP OpenView Network Node Manager commands, APIs, and ECS performance data.

Test Steps

Following the completion of TC028.001 through TC028.005, examine the History Log to ensure that all performance parameters which exceeded their configured thresholds have been recorded.

Using APIs provided by CSS, ensure that the Performance Management Application Service can send selected ECS performance data to the History Log.

Using APIs provided by CSS, ensure that the Performance Management Application Service can retrieve the following science algorithm performance data from the History Log:

- o algorithm name
- o algorithm version
- o start time
- o stop time
- o CPU utilization
- o memory utilization
- o disk reads
- o disk writes

Using HP OpenView Network Node Manager commands, extract summarized site information from logged performance data.

Verify that the EMC PMAS can request and receive performance and summarized performance data from the site PMAS and other external systems.

Verify that the site can send summarize data to the EMC PMAS.

Test Outputs

The expected results of this test include the ability to write and retrieve all selected performance management data to and from the History Log. Performance and summarized performance data from the performance data at the local sites.

Success Criteria

This test will be deemed successful when all selected performance management data has been properly written to and retrieved from the History Log.

Assumptions and Constraints

It is assumed that TC028.001 through TC028.005 have been successfully completed.

4.12.7 Test Case 7: Performance Trending (TC028.006)

This test case will demonstrate the ability of the MSS Performance Management Application Service to extract and graph from the History Log the measured values for any performance metrics gathered for specified network objects over a specified period of time.

Test Inputs

Inputs to this test case include HP OpenView Network Node Manager commands, ECS performance data stored in the History Log, and History Log populator scripts.

Test Steps

Following the completion of TC028.001 through TC028.006, examine the History Log to ensure that performance data exists.

Use History Log populator scripts to enter additional performance data covering approximately a two-year period.

Using HP OpenView Network Node Manager commands, extract performance metrics covering a two-year period.

Using HP OpenView Network Node Manager commands, generate a graph of the performance metrics extracted above.

Repeat the above two steps for a five-minute interval.

Repeat using the same start and stop times (null interval).

Test Outputs

The expected results of this test include the ability to extract and graph all selected performance management data from the History Log for the selected time period.

Success Criteria

This test will be deemed successful when all selected performance management data has been properly retrieved from the History Log and graphed for the selected time interval. An error message should be displayed if a null interval is selected.

Assumptions and Constraints

It is assumed that TC028.001 through TC028.006 have been successfully completed.

4.12.8 Test Case 8: Performance Testing (TC028.007)

This test case will demonstrate the ability of the MSS Performance Management Application Service to maintain and perform operational network performance benchmark test procedures. The results should also be maintained.

Test Inputs

Inputs to this test case include HP OpenView Network Node Manager commands and operational benchmark test procedures.

Test Steps

Ensure that the MSS Performance Management Application Service operational network performance benchmark test procedures reside in their designated location.

Perform all operational network performance benchmark test procedures.

Examine test results for any discrepancies.

Repeat all tests several times, and compare the results.

Introduce error conditions into the network, then re-run the operational network performance benchmark test procedures.

Test Outputs

The expected results of this test include the operational network performance benchmark test results.

Success Criteria

This test will be deemed successful when all operational network performance benchmark tests pass under normal network conditions. If any error or warning conditions exist on the network, they should be flagged.

Assumptions and Constraints

None.

4.12.9 Test Case 9: Performance Reporting (TC028.008)

This test case will demonstrate the ability of the MSS Performance Management Application Service to gather performance data and generated statistics and report them to the M&O staff and to the SDPS sybsystem. The performance management application service will also be capable of receiving and responding to requests from the SDPS subsystems.

Test Inputs

Inputs to this test case include performance data, performance statistics and resource utilization information.

Test Steps

Initialize HP OpenView.

Demonstrate the ability to graphically display the operational state of managed objects through HP OpenView.

Demonstrate the ability of the PMAS to calculate statistics for: a. Mean Down Time (MDT), b. Mean Time Between Maintenance (MTBM); (Mean Time Between Preventive Maintenance (MTBPM) and Mean Time Between Corrective Maintenance (MTBCM)) and c. Mean Time to Repair (MTTR).

Verify that the above statistics are stored in a repository accessible by the M&O Staff.

Demonstrate, as an M&O staff user, the ability to display in tabular and graphical formats selected performance statistics.

Print the statistics.

Verify that the PMAS is capable of receiving system resource utilization information requests from SDPS Data Processing Subsystem, SDPS Data Server and Data Processing Subsystems and SDPS Client subsystem.

Verify that the PMAS is capable of providing CPU utilization, memory utilization and disk I/O's to the SDPS Data Processing Subsystem, SDPS Data Server and Data Processing subsystems, and SDPS Client subsystem.

Verify that the PMAS is capable of receiving resource utilization information requests from the SDPS subsystem.

Verify that the PMAS has the ability to generate reports of the collected management data.

Verify that these reports can be redirected to the console, a disk file and a printer.

Test Outputs

Outputs include performance statistics and current resource utilization information. Reports of the management data in a variety of outputs.

Success Criteria

This test will be deemed successful when the resource utilization is provide by the MSS performance management application service and the SDPS subsystem can receive it.

Assumptions and Constraints

None

4.12.10 Test Case 10: Network Management Test (TC028.010)

This test case demonstrates that the Inter networking devices do event notification of relevant networking events. The test will be conducted in the EDF using facilities that emulate Release A facilities as closely as possible.

Test Inputs

Network manager commands to enable network device event notification.

Test Steps

1. Run network benchmarks with network event logging turned on.
2. Use network manager to requests various types of event data from network devices.
3. Introduce anomalies into the system, causing the failure or interruption of various network devices.

Test Outputs

Logs and alarms showing recorded event data.

Success Criteria

Log and alarm data consistent with the above test steps. No spurious alarm or log data.

Assumptions and Constraints

This functionality will be further verified in other build/thread tests since Inter networking will be a part of most other tests.

4.13 Fault Management Thread Test (TC029)

Fault Management addresses the detection, isolation, diagnosis, and the recovery from a fault condition in a managed object, to the restoration of the affected system or service to an operational state. The Managed Objects in Release A for which Fault Management is provided include network devices, operating systems, peripheral devices, processes, applications (to include algorithms) and databases. These managed objects include those of SDPS and CSMS.

The Fault Management Application Service (FMAS) comprises the following functional sub-services:

- Fault Definition and Setup
- Fault Detection and Notification
- Fault Diagnosis, Isolation and Identification
- Fault Recovery
- Reporting

Fault Policies and Procedures must demonstrate the proper policies and procedures necessary for fault identification and the subsequent recovery or corrective actions employed to recover from the fault. These policies will flow down from the EMC to the sites for implementation.

The Objective of this thread is to verify the before mentioned functional sub-services by demonstrating each of the sub-service requirements successfully.

Special resource requirements:

- DCE
- HP OpenView
- XRunner/LoadRunner

This thread contains 7 test cases.

4.13.1 Test Case 1: Fault Definition and Setup (TC029.001)

The purpose of the Fault Definition and Setup test is to demonstrate the management framework's ability to create and display graphical representations of network topologies. To organize the given network topology into a hierarchy of maps.

The FMAS will be tested to demonstrate the capability to perform the following functions:

a. define fault categories

b. assign faults to categories

c. assign severity levels to faults

FMAS must demonstrate the capability to provide the management data access service with a configurable lists of fault categories that specify whether to enable or disable in the logging of fault notifications for that fault category. FMAS must demonstrate the capability to enable or disable the display of fault notifications received from a specific managed object based on the fault category assigned to that fault and provide the capability to specify additional information to be added to a disk log file, based on the fault category, when the notification of a fault is received.

FMAS will also be tested to have the capability to establish, view, modify and delete defined thresholds on the performance metrics it measures.

Test Inputs

Test inputs include the SNMP managed objects that display the following graphical representations of a given network topology:

a. routers

b. communication lines

c. hosts

d. peripherals

e. applications

Test Steps

Graphic Topology verification

1. Initialize HP OpenView.
2. Verify that a map depiction of the network topology is accurately displayed.
3. Verify that the lower level topologies include hosts, routers, communication lines, peripherals, applications.
4. Verify their status condition.
5. Double-click on the available icons to verify that the lower level submaps exist and are accurately displayed.

Fault category verification

1. Define a fault category.
2. Assign specific faults to the defined category.
3. Assign severity levels to each fault.
4. Verify definitions, assignments and priority level.

Enable/Disable fault notification verification

1. Select OpenView management data access menu.
2. Verify configurable lists of fault categories from received fault notifications.

3. Select a specific fault.
4. Verify specification of enable or disable status logged for fault category.
5. Change fault category enable/disable status.
6. Verify status changed.
7. Add additional information to the fault disk log file (if applicable).

Performance threshold metrics

1. Display Performance Metrics menu.
2. Verify viewing of threshold settings.
3. Modify threshold settings.
4. Verify modification of threshold.
5. Delete threshold.
6. Verify threshold definition deleted.

Test Outputs

The expected results of this test include an accurate map display of the operational network with lower level maps including, individual sites, workstations and network topologies. Also, a successful demonstration of the fault management functions described in the test inputs.

Success Criteria

This test will be deemed successful when maps reflecting the network topology are displayed and the fault management requirements are successfully demonstrated.

Assumptions and Constraints

None.

4.13.2 Test Case 2: Fault Detection and Notification (TC029.002)

The purpose of this test case is to test the detection of a fault performed in two ways: by polling an attribute of a managed object and by the receipt of a notification from another entity. Fault detection may be accomplished by the FMAS itself for network devices, or by an agent for defined managed objects to include processes, databases, peripheral devices, or by an application (error conditions internal to an application).

The FMAS will be tested to demonstrate the capability to provide several mechanisms for the notification of a detected fault. These include visual indications/notifications of changing an icon color, displaying a message in a pop-up notification window, logging the notification to a disk log file (with optional operator-specified information), and generating audible alerts. All fault notifications must be logged for the purposes of record keeping, report generation and post processing.

The FMAS will be tested to demonstrate the capability to generate a fault notification when a defined threshold is exceeded and to receive notifications from SNMP agents and applications.

The EMC fault management application must demonstrate the capability to receive and/or request notifications of detected faults and degradation of performance data and be capable of receiving summarized fault notification and performance degradation data from the Site fault management applications and any other external systems as defined in the external systems requirements Section 5.1. Logging services will be tested for recording each detected fault.

FMAS will be tested to demonstrate the capability to generate the following types of notifications for detected faults:

a. Color change for icon display
b. Message in a pop-up notification window
c. Disk file logging the following fault information
    1. fault type
    2. date/time of fault occurrence
    3. source IP address of the notification
    4. fault data received with notification
    5. operator-defined descriptive text
d. Audible alert

FMAS must be capable of maintaining a list of external providers, M&O operators and applications to be notified in the event that a specified fault is detected. A registered recipient must be capable of receiving fault notification from FMAS and FMAS will also be tested to be capable of generating a fault notification within a maximum of five minutes of fault detection.

Test Inputs

The test inputs include demonstrating that the FMAS has the capability to poll for the detection of fault and performance information, by polling network elements at a frequency that 's defined in the system and receiving fault notifications from those elements, due to faults.

The following types of failures will be tested for proper detection by the FMAS:

a. communication software version mismatch errors
b. communication software configuration errors
c. communication hardware errors
    1. unreachable host
    2. unreachable router
    3. communication link failures/errors
d. protocol errors

e. performance degradation due to exceeded thresholds
f. peripheral errors
g. database errors
h. application errors
    1. missing process (Application or COTS product)
    2. process in loop

Test Steps

Fault detection polling

1. Bring-up network graphical display on OpenView.
2. Disengage network element (cause failure).
3. Verify receipt of element failure detection from network display/alarm.
4. Verify correct failure detected.
5. Verify fault detected within time frequency set in system.
6. Repeat for all element failure types.

Fault notification for exceeding threshold limits

1. Display Performance Metrics menu.
2. Modify threshold settings to cause immediate failure.
3. Cause threshold to be exceeded for SNMP agent.
4. Verify receipt of threshold failure detection from network display/alarm.
5. Repeat for application failure.
6. Verify correct failure notification received.

Performance degradation detection and notification

1. Create performance threshold.
2. Cause degraded network performance.
3. Verify fault notification received from Site management and/or external systems.
4. Verify correct failure notification received.
5. Verify fault notification is recorded by fault logging services.

Fault notification type verification

1. Generate fault notification by network element failure.
2. Verify proper color change for icon displayed.
3. Verify message pop-up notification window received.

4. Verify audible alert received.
5. Verify disk log file recorded the following information for the fault received:
    a. fault type
    b. date/time of fault occurrence
    c. source IP address of the notification
    d. fault data received with notification
    e. operator-defined descriptive text

Fault support registration list verification

1. Create a fault distribution list of support providers.
2. Generate fault notification by network element failure.
3. Verify correct failure notification received by all registered recipients within a five minute time period.

Test Outputs

The expected results of this test include a successful demonstration of the fault management functions described in the test inputs.

Success Criteria

This test will be deemed successful when the fault management requirements are successfully demonstrated.

Assumptions and Constraints

None.

4.13.3 Test Case 3: Fault Diagnosis, Isolation and Identification (TC029.003)

The purpose of this test case is to demonstrate that the Fault Management Application Service can provide the required mechanisms to facilitate the proper diagnosis, isolation and identification of a fault. These include diagnostic tests, vendor-provided diagnostics and the disk log files that contain vital diagnostic information. The FMAS debugging aid must be capable of performing:

a. packet tracing of protocols used in ECS
b. periodic testing of all ECS communication links from site to verify operational
c. verifying operational status of a host
d. periodic diagnostic for isolation and identification of fault

FMAS must demonstrate the capability to execute vendor diagnostics in order to diagnose faults traced to hardware equipment. Note: diagnostics will be limited to vendor functionality and availability.

FMAS will be tested to demonstrate the capability of sending gathered isolation, location, identification and characterization of reported faults data to the level of subsystem and equipment to the site FMAS and any other external systems as defined in Section 5.1. FMAS at the sites must be capable of demonstrating all the before mentioned faults including software faults, and identify the nature of the faults detected within the site at he levels of subsystem, equipment and software. FMAS will also be tested for the capability to retrieve records of detected faults.

Test Inputs

The test inputs to this test case include testing FMAS capability to identify routes between selected pairs of hosts on the ESN. FMAS must be capable of providing utilities that will perform diagnostics and testing for the following isolated faults:

a. connectivity between ECS hosts and ECS routers

b. ability to reach hosts and routers

c. availability of network services at hosts

Test Steps

Fault identification and isolation verification

1. From OpenView network topology display, verify all ESN system connectivity between hosts and routers within network.
2. Verify network services available at designated hosts.
3. Select OpenView protocol analyzer to display packet tracing feature.
4. Verify trace feature operational and functional.
5. Set debugging tool for periodic testing of communication links from site.
6. Verify period tests operational.
7. Verify operational status of host from OpenView network display.

Vendor diagnostic verification

1. Select vendor diagnostics.
2. Execute diagnostics for vendor hardware (i.e., HP, SUN, DEC, IBM, etc.).
3. Verify proper fault isolation and identification.

Fault isolation and identification data distribution

1. Create a fault distribution list of support providers.
2. Generate fault notification by network element failure.
3. Verify all fault data gathered is sent to the levels of subsystem , equipment to the site FMAS, and any other external systems as defined in Section 5.1 of the requirements.
4. Retrieve records of detected faults from other subsystem levels.

5. Verify records retrieved are correct.

Test Outputs

The expected results of this test include a successful demonstration of the fault management functions described in the test inputs.

Success Criteria

This test will be deemed successful when the fault management requirements are successfully demonstrated.

Assumptions and Constraints

None.

4.13.4 Test Case 4: Fault Policies and Procedures (TC029.004)

This test case demonstrates that the minimum policies and procedures will be capable of fault management.

Test Inputs

Test input requires the FMAS to be able support, maintain, and update the system fault management policies and procedures which include:

a. Fault Identification

b. Fault priorities

c. Recovery and corrective actions

FMAS will be tested to be capable of receiving fault management policies and procedures from the EMC and to be capable of interfacing with the Configuration Management Application Service to schedule a change in the configuration of the site when such a change is deemed necessary, to recover from a fault.

Test Steps

Policy and procedure verification

1. Access the system fault management policy and procedure files.
2. Verify that the Configuration Management Service is flexible enough to make configuration changes when deemed critical, to recover from a fault, according to the stated policies and procedures.

Test Outputs

The expected results of this test include a successful demonstration of the fault management functions described in the test inputs.

Success Criteria

This test will be deemed successful when the fault management requirements are successfully demonstrated.

Assumptions and Constraints

None.

4.13.5 Test Case 5: Fault Recovery (TC029.005)

The purpose of this test case is to test the recovery procedures that will be initiated in order to restore the system to an operational state. These recovery procedures may be simple (the resetting of file permissions and restarting an application that aborted due to an error accessing a file), or more involved (scheduling corrective maintenance of failed equipment). In the latter case, some coordination with the Configuration Management Application may be necessary. Once the fault condition has recovered, the failed component may be restored to an operational state. FMAS must demonstrate the capability to provide the specification and execution of action routines in response to the notification of a fault and be capable of passing parameters to the action routines. Automation support tools will be verified as being utilized for the support of recovery from faults within the site.

Test Inputs

Test inputs include verifying that the EMC FMAS coordinates the recovery from conditions of degradation of performance and faults with the sites and external network service providers, also verifying the coordination, as necessary via directives and instructions, of the recovery from faults reported from a site.

Test Steps

Coordinate between the EMC FMAS, Site and external systems a fault notification recovery procedure which provides the specification and execution of action routines in response to the notification of a fault and passes parameters to the action routines.

Automation support tools must be utilized for the generation of directives and instructions for recovery from faults within the site.

Test Outputs

The expected results of this test include a successful demonstration of the fault management functions described in the test inputs.

Success Criteria

This test will be deemed successful when the fault management requirements are successfully demonstrated.

Assumptions and Constraints

None.

4.13.6 Test Case 6: Fault Reporting (TC029.006)

The purpose of this test case is to test the capability of FMAS to gather fault data that can be reported to M&O staff and external service providers in a graphical and tabular format via the MUI. Fault Management Application Service must also demonstrate the capability to provide the M&O staff with the ability to select and generate fault statistics (real-time and historical) for operator-selectable managed objects. These statistics must be displayable in either a tabular or a graphical format.

Test Inputs

Test inputs require FMAS to demonstrate the capability to generate, on an interactive and scheduled basis, reports on performance/error data, that it has been configured to collect along with the capability to build histories for different types of errors and events detected, for the purpose of analysis.

Test Steps

1. From OpenView bring up the performance analysis menu.
2. Create thresholds that will reflect a very unstable system.
3. Create scheduled network probing periods.
4. Verify report generation for network performance and error data collection.
5. Demonstrate the ability to redirect the reports to the console, to the disk file, and to the printer.
6. Verify logging of records reflecting histories for different types of errors and events detected.

Test Outputs

The expected results of this test include a successful demonstration of the fault management functions described in the test inputs.

Success Criteria

This test will be deemed successful when the fault management requirements are successfully demonstrated.

Assumptions and Constraints

None.

4.13.7 Test Case 7: Management Agent (TC029.007)

The purpose of this test case is to test the functionality associated with the MSS Management Agent Service.

Test Inputs

Inputs to this test case include an agent for ECS host systems and applications and a driver to simulate two agents communicating.

Test Steps

Verify that the Management Agent Service provides an ECS management agent for ECS Host systems.

Verify that an extensible management agent is provided for ECS applications.

Verify that through an ECS domain manager agent multiple ECS management agents can coordinate and communicate.

Test Outputs

Communications between multiple agents.

Success Criteria

This test will be successful when the extensible agents can manage network devices, Host systems and the domain manager agent can coordinate and communicate between multiple agents.

Assumptions and Constraints

None.

4.14 Accountability Management Thread Test (TC030)

The purpose of this thread is to verify the functionality of the Accountability Management Service, which provides two basic functions: user registration and audit trails. The user registration will allow new users to have privileges other than those of guest users and the audit trails will provide a record of previous events to reconstruct past activities. To verify the DCE user registration and commands required to register a DCE user.

The objective of this test is to verify that a user, who wishes to become an ECS user, can self-register. Verify that a user has three ways to register and for each way the user is given a response to his request. Ensure that self-registration does not open an account. Verify audit trails in order to recreate past events.

Special resources required for this thread test include:

- o DCE cell(s)
- o MUI

This thread contains 8 test cases.

4.14.1 Test Case 1: DCE User Registration (TC030.001)

The purpose of the DCE User Registration test is to verify the underlying functionality necessary to register a DCE user. The DCE security database contains all the security relevant information about all the entities within the Registry. The registry is divided into five parts: Principals, Groups,

Organizations, Accounts, and Policies and Properties. The principal is required for any authenticated conversation within DCE. Principals can be grouped together. The group is used to determine access control to DCE objects. The organizations are additional groupings of principals and they affect the privileges of the user. Accounts are made up of principal name, group name and organization name. Accounts are required for any user wishing to interact with the registry and provide principals with authentication characteristics and network identity information. Policies and Properties govern the behavior of and access to the registry.

Test Inputs

Inputs to this test case include the use of rgy_edit commands to modify the security registry server.

Test Steps

Logon to the cell as the DCE administrator

Using rgy_edit commands enter the information required for a new user

Verify that the new user ID is operational and that only the assigned privileges are accessible

Set the ID life span for X time

Verify that when X time is reached the ID is destroyed

Using rgy_edit modify the authentication and registry properties

Verify that the new policies are in place

Using rgy_edit conduct organization management

View a group

Verify that the group reflects the new organization

Logon to the cell as a the user that was just entered

Verify that the ticket information has been granted

Test Outputs

Outputs to this test case include outputs of the group, principal and organization structures to view the user privileges.

Review the process required for entering users into the DCE security server

Verify the procedures for determining valid/invalid passwords

Success Criteria

This test will be deemed successful when all of the rgy_edit commands have been demonstrated and the user registration process has been examined for completeness.

Assumptions and Constraints

Will be provided with a DCE Administrator account to enter information into the security server. The requirements for these COTS provided capabilities will be demonstrated in this test case. Further implicit regression testing of these functions will occur during thread tests. The latter will provide GUI and MUI that will exercise the underlying DCE functions described in this test case.

4.14.2 Test Case 2: Registration (TC030.002)

The purpose of the Registration test is to demonstrate the available functionality provided to the user for register as a valid ECS user. Verify the capability of three unique ways for a user to register. Verify that the registration does not automatically lead to the creation of a new ID (ID includes both logon name and password). This test case addresses users requesting special privileges. Guest users or users requesting non-restricted ECS services will be tested separately.

Test Inputs

User registration in three ways: via on-line user registration, by activating the Register function within the ECS Client Toolkit and completing and submitting a New User Registration package available at the site. Mail message indicating acceptance or denial of the ID.

Test Steps

Guest user accesses the bulletin board service either as a stand alone application or through the ECS Client

Accesses the on-line user registration form

User completes the form

User submits the form via E-mail

User receives an E-mail from the ECS operations staff indicating if the account has been accepted or denied (the request is evaluated based on criteria prescribed in ECS policies)

Guest user accesses the ECS Client Toolkit either as a stand alone application or through the ECS Client

User accesses the Register function

User completes the registration process

Request is evaluated by the ECS operations staff based on criteria prescribed in ECS policies)

Users receives a message indicating if the request has been approved or denied

Potential user visiting a site is interested in becoming an ECS user

Potential user fills out the New User Registration package

Submits the package

Package is reviewed by ECS operations staff based on the criteria prescribed in ECS policies

User receives mail indicating if the account has been approved or denied (if the user has been given an id, the user password will be in a presealed envelope and mailed to the user).

Test Outputs

The test outputs for this test case include US mail notification. Addition of new users.

Success Criteria

This test will be deemed successful if a guest user can request an ECS user account by either registering through the bulletin board service or through the ECS Client Toolkit. If a potential user (could be guest user) can register to become a valid ECS user by filling out a New User Registration form located at the site.

Assumptions and Constraints

Approval to become a registered user is a manual process and will be conducted at each site. User has access (as a guest) to bulletin board service. All requests are evaluated on criteria based on prescribed ECS policies. Only requests with special privileges will require an operators approval.

4.14.3 Test Case 3: Guest Registration (TC030.003)

The purpose of the Guest Registration test is to demonstrate the available functionality for a guest user to register with ECS.

Test Inputs

User registration as a guest user.

Test Steps

Initialize ECS

Logon as “Guest”

Verify that the user can access ECS

Verify that the Guest user is provided the appropriate privileges

Test Outputs

Screen notification indicating which functionality the guest user can perform and which he can not.

Success Criteria

This test will be deemed successful if a guest user can access the ECS with applicable privileges.

Assumptions and Constraints

None.

4.14.4 Test Case 4: Frequent User Registration (TC030.004)

This test case will verify that user information will be maintained for users who do not require special privileges, but regularly access ECS.

Test Inputs

Registration of a frequent user.

Test Steps

Logon to ECS

Complete the user registration for a user who does not require special privileges

Verify that the ID can be created without going through the ECS operational staff

Confirm creation of ID by performing a successful logon to ECS with the new ID

Verify that the applicable privileges have been granted

Test Outputs

The test outputs include: ECS access indicating valid ECS ID with applicable privileges.

Success Criteria

This test will be deemed successful when a user who frequently uses the system can register for limited privileges without going through ECS production staff revision.

4.14.5 Test Case 5: Contents (TC030.005)

The purpose of the Contents test is to verify that all of the appropriate information is contained in the user notification and user profile. The contents are based on the documented User Registration Requirements.

Test Inputs

User registration and US mail notification to the user indicating acceptance or denial of the account. ECS operations staff logon and password with privileges to view the user profile.

Test Steps

Retrieve a US mail message that was sent to a user in the Registration test case.

Display the contents of the message

Verify that the message includes: information regarding the initial system access procedures (including initial password), priority information, and authorized services

Log into ECS as an operations staff member with privileges to view the user profiles

Display the contents of the user profile

Verify that the user profile includes: Name of the principal investigator (including affiliation), full mailing address, telephone, E-mail address, names and addresses of co-investigators if separate logon accounts are required and product shipping address. Also included when applicable, name of the project for which the account is required, including objective, duration, data requirements, and information to be derived.

Test Outputs

Screen display or printouts of US mail notification, user profile and contents of user profile database.

Success Criteria

The test will be deemed successful when the US mail notification and user profile are verified to ensure that all of the required contents are included within these records.

Assumptions and Constraints

The completion of a successful account request from the Registration test case. User profile is created based on the information provided by the user. The contents of the file are based on the User Registration requirements.

4.14.6 Test Case 6: MSS Accountability Management (TC030.006)

The purpose of the MSS Accountability Management test is to verify that all of the appropriate information is contained within user profile database. The contents are based on the User Registration Requirements as outlined in Section 5.2.5 of the Communications and System Management Segment (CSMS) Requirements Specification for the ECS Project. To ensure that the service is capable of receiving user profile records and to create a new user account when a new record is added to the user profile database.

Test Inputs

Inputs to the MSS Accountability Management test include a logon and password for a operations staff members with the needed privileges.

Test Steps

Log into ECS as an operations staff member with privileges to access the user profile database and to enter a user profile

Display the contents of the database

Verify that the database includes the following information for each registered user: name, user ID, password, assigned privileges, mailing address, telephone number, product shipping address, E-mail address, Organization (optional), Project Affiliation [project name and project principal investigator (both optional)] and user group

Enter a user profile for a new user

Verify that the service received the new user profile

Verify that a new ID is created for every new user profile entered

Verify the process that is in place to enlist a new user

Verify that the new ID contains the appropriate user information

Verify tht the accountability management service can generate reports from the collected management data and that these reports can be output to the console, a disk file and/or a printer

Test Outputs

A display (dump) of the user profile database contents. The creation of a new user account.

Success Criteria

This test will be deemed successful when the user profile information entered from the ECS site operational staff is received by the service an ID is created based on this information and the user profile database contains all of the attributes listed above.

Assumption and Constraints

The completion of a successful account request from the Registration test case. The reception of the user profile records entered by the operations personnel and entrants to the user profile database containing the appropriate contents. The contents of the file are based on the User Registration requirements contained within the Communications and Systems Management Segment (CSMS) Requirements Specification for the ECS Project (304-CD-003-001). User registration procedures will be documented at the time of testing.

4.14.7 Test Case 7: User Audit Trail (TC030.007)

The purpose of the User Audit Trail test is to verify that the audit is tracking user access data such as: class of user, user ID, duration of each session, time of each access or attempt to access and type of files accessed.

Test Inputs

Inputs to this test case include user logon and password with privileges to view the contents of the management database. SDPS records storing the data to be ingest to the management database. Telnet, FTP, rlogin and finger sessions. Records generated by the SDPS applications.

Test Steps

Logon as a user with root privileges for the MSS Accountability Management Service

Verify that the service is capable of retrieving information in the records generated by the SDPS Data Server, Data Processing, and Client Subsystem

Verify that the service is capable of querying the user activity data stored in the management database

Verify that information for a particular user or data item can be abstracted from the database

Telnet into an ECS host

Verify that the information for the telnet session was logged

FTP a file to an ECS host

Verify that the information for the FTP session was logged

Remote login to an ECS host

Verify that the remote login session was logged

Finger a user on an ECS host

Verify that the finger session was logged

Verify that the M&O staff is able to obtain audit information via the MUI service

Test Outputs

The outputs for this test case include a printout/screen dump of the management database. Screen notification of successful telnet, FTP, rlogin and finger sessions.

Success Criteria

This test will be deemed successful when the information stored in the SDPS records is retrieved and queried by the service. The service performs a query for a particular user of data item. Telnet, FTP, rlogin and finger sessions were logged by the service and M&O reported audit information via the MUI service.

Assumptions and Constraints

The information will be logged, each time a user attempt to logon or access one of the SDPS services, by the SDPS subsystem. The sub-service will coordinate with the security services for security violations and for managing users account audits.

4.14.8 Test Case 8: Data Audit Trail (TC030.008)

The purpose of the Data Audit Trail test is to verify the process of orders as they are processed through the system. To ensure that upon completion of the order, a record of the completion will be entered into the database, which includes: the user who ordered the product, the product ordered, the media type requested, the name of the completed activity, and the duration of time from placement of order to completion of order.

Test Inputs

Placement of a data order. Searching of local history logs.

Test Steps

Logon as a user capable of retrieving information from the SDPS generated records and the management database

Retrieve the data processing information (instrument used and date/time of ingest or algorithm used (name and version) and date/time of processing)

Verify that the information could be retrieved

Verify that the user can query the management database: for all data processing information stored in the management database, retrieving all data processing information logged for a specific data item and accepting queries for the status of a particular ordered data item from the SDPS Client subsystem.

Verify that the service is capable of interfacing with the SDPS subsystems to determine the status of a data order

Verify that the service can return the status to SDPS

Verify that the service can search the local history logs to find processing data for an ordered data item

Test Outputs

Outputs to this test case include: printout (screen dump) of data processing information, queries based on test steps above and outputs of history log data.

Success Criteria

This test will be deemed successful when all of the desired data is reviewed for completeness.

Assumptions and Constraints

That the SDPS records were ingest to the database as a result of the User Audit Trail test.

4.15 Management Services Build Test (BC031)

The Management Services Build represents the integration of the CSS, ISS and MSS functionality for Release A. This test is an aggregation of the Internetworking, GUI Based Session, Directory Service, Distributed File Service, E-mail/Bulletin Board Service, PGS Toolkit Interface, Systems Logistics Management, Fault Management, Accountability Management, Security Management and Network Security threads, as well as the CSMS IR-1 Communications, CSMS IR-1 Management Framework, Communications and System Security Builds. The CSMS IR-1 Communications Build is an aggregation of the CSS and ISS functionality that carries over into Release A from IR-1. The CSMS IR-1 Management Framework Build is an aggregation of the MSS functionality that carries over into Release A from IR-1. The functionality regression tested from IR-1 includes: file transfers, communication via the internet, demonstrate ACLs, communications with external interfaces, fault recognition and notification and CM. Release A functionality tested includes regression testing of all of the threads outlined in Section 4.

The objective of this test is to verify that all of the previously tested functionality, based on the requirements as outlined in the Communications and Systems Management Segment (CSMS) Requirements Specification for the ECS Project, is still available upon integration of the Management Services Build

Special resources required for this thread test include:

- Operational DCE cell
- Access to workstations at DAACs, SCFs, and External ECS Users
- LoadRunner / XRunner
- Sensor Data Processing Facility(SDPF) simulator
- TRMM Science Data and Information System (TSDIS) simulator
- NOLAN emulation, for example protocols
- Emulated IR-1 DAAC configuration
- HP OpenView
- Network analyzer
- NSI and ESN V0 connections
- Isolated processor for virus detection testing
- randomly selected set of viruses
- Security Registry and ACL file maintenance programs
- Network device, processor, and application management agents
- Security Compliance Test Suites
- Network traffic generator
- Network device configuration interfaces

This thread contains 13 test cases:

4.15.1 Test Case 1: IR-1 Communications Regression (BC031.001)

The purpose of the IR-1 Regression test case is to demonstrate that upon the integration of the ISS and CSS functionality from IR-1 the software will still function as expected in Release A. This functionality includes: communicating over variety of interfaces, ability to transfer files from DAAC to DAAC to SCF to EDF and communication amongst the DAACs via E-mail.

Test Inputs

Inputs to this test case include various combinations of valid/invalid ID and valid/invalid password, valid admin ID and password, valid add, change and delete registry commands, ability to access and modify directories, time checks using DTS. RPC calls within a host and from host to host will also be tested. A file to be transferred and a simple E-mail message.

Test Steps

Verify which of the interfaces exist

Through simulation or use of non operation IR-1 data, verify that the interfaces are functional

Run an XRunner script that calls a file with various valid/invalid IDs/passwords

Upon successful login, call another XRunner script to change the users password, logout and login with the new password

Logon as the DCE Administrator

Add, change, and delete commands to/from the security registry

Set up a cron job to retrieve the time from each of the workstations in the operational cell and store them in a file

Inspect the file to insure that all of the times are in sync

Set up a workstation to run as the server

Set up all of the workstations to be clients (including the server workstation)

Initialize the server

Initialize communications between client and server

Create a file equivalent in size to an SCFs algorithm

Using ftp transfer the file from SCF to each of the DAACs

From the DAAC(s) return an E-mail message to the SCF verifying that the file has been received

Send an E-mail message between the DAACs (plus EDF), making sure that each site sends/receives at least one message

Test Outputs

Test outputs include data products/outputs produced by the emulation. Screen outputs showing the success or failure of the logon/logoff attempts. Response times of each logon and logoff event. Network monitor output showing the data transmitted between client and server. Event log data. Flat file showing the times recorded during execution of the cron job. Screen outputs showing successful bindings between clients and server. Test outputs include the verification (visual) that a file had been transferred to the DAAC. The successful completion of an E-mail message.

Success Criteria

This test will be deemed successful when all of the detailed functionality is verified.

Assumptions and Constraints

It is assumed that the DAAC file system will be populated with a number of directories, subdirectories, data files, and other objects. All workstations are configured to transfer and receive mail messages via E-mail. If an SCF is not available we will simulate the SCF functionality for IR-1 SCF will be DCE clients. For IR-1, SCFs will be DCE clients. The Primary Investigator will be a DCE client. The PI will be responsible for distributing information among other scientists.

4.15.2 Test Case 2: IR-1 Management Framework Regression (BC031.002)

This test case regression tests the Management Framework Build previously tested in IR-1. IR-1 interface tests are described in Volume 1, Section 4.16 of the CSMS Segment I&T Plan.

4.15.3 Test Case 3: Communications Integration (BC031.003)

This test case is an integration of the Communications Services Build previously tested in Section 4.7. This test includes all of the thread which make up the Communication Services Build. The previous thread tests which will make up this test are described in Volume 1, Section 4.12 of the CSMS Segment I&T Plan and Sections 4.1 - 4.6 above.

4.15.4 Test Case 4: System Security Integration (BC031.004)

This test case is an integration test of the System Security Build previously tested in Section 4.10. This test includes an aggregation of the threads which make up the Communications Integration (Section 4.15.3) and the Security Management and Network Security threads (Sections 4.8 and 4.9).

4.15.5 Test Case 5: MSS Integration (BC031.005)

This test case is an integration test of the aggregation of the CSMS IR-1 Management Framework (previously tested in Volume 1, Section 4.16 of the CSMS Segment I&T Plan), Systems Logistics Management (Section 4.11), Performance Management (Section 4.12), Fault Management (Section 4.13) and Accountability Management (Section 4.11) threads. This test includes all of the threads which make up the Communication Services Build.

4.15.6 Test Case 6: General DBMS (BC031.008)

The purpose of the General DBMS test case is to demonstrate/inspect all of the available functionality associated with the DBMS available in the Release A time frame. To verify that the Monitor/Control Service successfully performs the statistical analysis and can log it into the database.

Test Inputs

Inputs to this test case include commands to initialize various DBMS functionality and data to perform statistical analysis.

Test Steps

Initialize the DBMS.

Verify that the DBMS requires security access control based upon userid, role and privileges for: database, database objects and database operations.

Demonstrate that the DBMS shall provide an SQL interface with query, update and administrative functions.

Inspect the Federal Information Processing System Publication to ensure compliance by the SQL-2.

Initialize the related CSS session-establishment service, verify that the DBMS can be accessed by or supported by the service.

Verify that a client/server paradigm is supported.

Generate ad hoc statistics from the management data.

Demonstrate the functionality for bulk data load and database backups (frequency, time, and type of backups).

Demonstrate on-line disk management functionality.

Verify the compatibility of the DBMS and the ECS management framework to support the importing of the ECS management framework data.

Verify that access structures are supported to improve the efficiency of retrieval of management data.

Verify data compression, space reallocated from deleted records and variable-length column storage.

Restore the database to a specific time, all or part.

Demonstrate the functionality associated with recovery.

While recording data issue and record a database checkpoint.

Run an audit trail to verify that all of the database activities have been recorded.

Perform statistical analysis by the Monitor/Control Service.

Verify that the statistical analysis performed by the Monitor/Control Service shall be capable of being stored in the management database for historical purposes.

Verify that the Statistical analysis is for average, median, maximum, minimum, ratios, rates and standard deviation.

Test Outputs

The outputs to this test case include: ad hoc statistics and reports, results of database queries, updated databases, database backups, archived data, recovered data, data compression and bulk loaded databases, and an audit trail outlining what has been done with the database. Statistical analysis and the results being stored in the management database

Success Criteria

This test will be deemed successful when all of the functionality associated with the data base has been demonstrated/tested/inspected and verified. Statistical analysis and logging of the data into the database.

Assumptions and Constraints

The Monitor/Control Service was successfully tested for statistical analysis.

4.15.7 Test Case 7: MSS Internal Interfaces test (BC031.013)

This test case will verify that all of the expected MSS internal interfaces have been met.

Test Inputs

Inputs to this test case include: an event, a message, time, file access, bulletin board, electronic mail, history log data, security events, performance events, request network protocol status, request network hardware status, etc. The SDPS and FOS interfaces and data will be simulated, since at the time of testing the actual interfaces will not be available.

Test Steps

Demonstrate the functionality of MSS to communicate with simulated SDPS and FOS entities and to pass the agreed upon data types as outlined in Tables 5.1-2 and 5.1-3 of the communications and System Management Segment (CSMS) Requirements Specification for the ECS Project (304-CD-003-002).

Verify the ability of the MSS interfaces between the LSM at the sites and the EMC at the SMC to communicate.

Send history log summary data, security events, fault events, performance events and registration data to the EMC from the LSM.

Verify that the EMC can receive and decipher the information.

Send data requests, policy directives, software distribution, and registry data to the EMC to the LSM.

Verify that the LSM can receive and decipher the information.

Send security events, fault events performance events, and registration data to the LSM from the LSM.

Verify that the LSM can receive and decipher the information.

Verify that the CSS API can send event logger, time, and a message to the MSS.

Demonstrate the ability of the CSS server to provide Electronic Mail, file access, bulletin board, virtual terminal, directory/naming, and security data to the MSS.

Demonstrate the ability of the MSS to send service requests to the CSS server

Demonstrate the ability of the MSS to request, from the ISS, network protocol status, network hardware status.

Verify that the ISS receives network protocol diagnostics, network hardware diagnostics, and router table maintenance from the MSS.

Verify that the ISS can send the MSS network protocol status data and network hardware status data.

Test Outputs

Test outputs include the successful interactions with all of the above interfaces.

Success Criteria

This test will be complete when the MSS has successfully communicated with all of the interfaces.

Assumptions and Constraints

None.

4.15.8 Test Case 8: MSS External Interface Scenario Test (BC031.012)

The MSS Interface Scenario Test verifies the ability of the MSS Subsystem to communicate with the various internal and external entities, as outlined in the Communications and System Management Segment (CSMS) Requirements Specification for the ECS Project (304-CD-003-002). In most cases, the internal and external entities will be simulated in the EDF. The data sets used will, as closely as possible, represent the data as outlined in Table 5.1-1 of the CSMS DID 304. [At this point communications between ECS and many of the interfaces are on going to determine exactly which data will be transferred, what protocol will be used and by which mechanism the data will be transferred.] The only interfaces established by the ICDs at this time have been man-in-loop and E-mail. Talks with Ecom are ongoing to determine which, if any, electronic interfaces will be implemented. Whatever interfaces are agreed upon and documented in an ICD will be simulated and tested.

Test Inputs

The inputs to this test case include a variety of different data sets representative of the data sets outlined in Table 5.1-1. Other inputs include simulators to emulate the various interfaces.

Test Steps

Setup a simulator to emulate the Ecom interface. Verify that data files, representative of the data files to be transferred between MSS and Ecom, can be transferred between the interface. Also, verify that these data files will be transferred using the protocol and mechanism as agreed upon by the MSS and the appropriate interface.

Repeat the following scenario for each of the appropriate interface outlined in Table 5.1-1, using the agreed upon mechanism, protocol and data sets.

Test Output

Outputs to this test case include the successful transfer of the data sets over the agreed upon protocol using the appropriate mechanism for each of the interfaces outlined in Table 5.1-1.

Success Criteria

This test will be deemed successful when communications between each of the interfaces and the MSS subsystem has been successfully emulated.

Assumptions and Constraints

All of the interfaces will be simulated in the EDF Testing Facility.

4.15.9 Test Case 9: LSM Scenario (BC031.006)

The purpose of the LSM Scenario test is to test, as much as possible the functionality of the LSM. By executing this scenario we hope to verify as many requirements as possible and regression test as much of the Release A management services functionality as possible. The testing will take place at the EDF in an environment that, as closely as possible emulates the planned production LSMs. DAAC and SMC functionality required to support LSM testing will also be emulated in the EDF to as closely as possible reflect the operational entities.

Test Inputs

Inputs to this test case include: the insertion of a faults, simulated data on the operational states of applications, operating system resources and network components, analyzed data compared with established criteria, adjusted measurement criteria. Other inputs include: insertion of a new security rule/policy, security intrusions, password audits and software and CCRs.

Test Steps

Enter a CCR using the Change Request Manager (CRM). Verify that the CCR goes through the proper procedures and that it is entered into the database. Verify that the CCR is then under local CM control and that it is associated with the site CCB. Verify, that if it impacts ECS, CSS is used to attach electronic copies of the proposed change. Verify using the CRM that reports can be generated regarding change requests associated with the local site and that the reports are made available to the appropriate offices via CSS file transfer service. Demonstrate using the Software Change Manager to execute all library operations, configure the site library to establish the branches for algorithm files and access permissions. Check the software into the site library with name, version, file types, format references, and file associations. Verify that the user who is submitting the new files has the appropriate permissions and privileges. Verify upon successful verification of the permissions and passwords that the new software versions are stored.

Initialize OpenView to monitor the network. Verify that the local fault management application service provides the capability to detect, diagnose, isolate and recover from faults that occur in the managed objects within ECS. Insert an unacceptable change in the state of a managed object causing a fault. Run diagnostic tests to determine the cause of the fault. Begin the initiation of corrective action to restore the system normal operational status. Provide the capability to generate notifications of fault conditions in and alert indicators in the event of defined thresholds being exceeded. Provide diagnostic information and the diagnostic tests that facilitate the isolation, location and the identification of the cause of the faults local to the DAAC. Incur a fault. Verify that the LSM recognizes the fault and that it places into action the necessary steps to recover from the defined faults.

Verify that the LSM is continuously gathering statistical and historical data, on the operational states of applications, operating system resources and network components, to analyze the data collected by comparing it with the established criteria, adjust measurement criteria or initiate other

corrective actions as necessary in order to ensure an optimal utilization of resources. Verify that the LSM is providing benchmarking and trends analysis of network component performance. Verify that the site performance management application service is collecting and processing the performance data local to the site and periodically sending it to the SMC.

Verify that the LSM provides security in three separate parts: network security (based on router address filtering), distributed communications security (Kerberos/DCE for real-time authentication exchanges), and host based security. Implement a new security rule into the LSM. Try to incur a security breach by breaking this rule. Verify that the LSM is capable of handling the situation. Try to log into the DAAC several times with an invalid password. Verify that the LSM is logging the intrusion attempts. Verify that a message is sent out to the other DAACs and the SMC indicating that someone has been attempting to intrude the system. Attempt to modify the routing tables used for address-based filtering with an invalid ID. Verify that you are unable to modify the tables. Attempt to modify the tables this time with a valid ID verify that the LSM updates the table. For each intrusion verify that notifications of security events and summary data are forwarded by the service to the SMC via electronic mail and the telephone. Produce reports for each of these activities.

Test Outputs

Electronic copies of changes required by the CCR, summary reports about change requests associated with each site, indication (either screen notification or E-mail) that a fault has occurred, logs containing historical and statistical data, local performance data periodically sent to the SMC, message sent out to other DAACs and SMC notifying them of intrusion attempts and reports listing security events and intrusion notification.

Success Criteria

This test will be deemed successful when: a CCR is entered into the system and the proper steps/procedures are followed throughout closure, the new software is checked into the CM tool and configured properly, when a fault occurs and the fault is recognized and the necessary steps are taken to recover the fault, when the appropriate performance data generated locally is periodically sent to the SMC, intrusion attempts are logged and the SMC is appropriately notified of the attempts.

Assumptions and Constraints

Assume Performance test cases complete.

4.15.10 Test Case 10: SMC Scenario (BC031.007)

The purpose of the SMC scenario test is to, regression test Release A management services functionality. The testing will take place at the EDF in an environment that, as closely as possible emulates the planned production SMC. The discussed LSM function will be emulated in the EDF to as closely as possible reflect the operational LSM.

Test Inputs

Inputs to this test include: various combinations of valid/invalid password/ID combinations, a fault, performance data, logon not meeting all of the security criteria, CCR, and a new software version.

Test Steps

Inject a fault at the emulated LSM located in the EDF. A variety of faults will be incurred in a variety of ways. Upon appropriate action performed by the LSM and when the predefined conditions (to cause SMC notification) have been met, verify that the SMC receives appropriate notification of the fault condition from the Fault Management Service at the emulated LSM. Verify that the SMC notifies the other emulated LSMs indicating that a fault has occurred and to ensure a quick resolution so that the fault will not occur at another emulated DAAC. Produce reports based on the information it collects and receives from the various Fault Management Application Services. Verify that the site Performance Management Application Service collects and processes performance data local to the site and periodically sends the information to the SMC. Evaluate the system-wide trends and system-level performance analysis based on the performance management information obtained from the LSMs. Produce the system wide summary performance reports and notifications of performance metrics exceeding established thresholds.

Define the security directives and guidelines. Distribute these guidelines to all of the DAACs. Log into an emulated DAAC (at the EDF) not meeting all of the criteria defined in the security directives and guidelines by the SMC. Verify that the user gets flagged and that the information is recorded at the local site. Verify that for a security violation the SMC is notified. Verify that the SMC coordinates the recovery from detected security breaches at the sites and external systems. Verify that the SMC notifies the other DAACs of the attempted security breach. Upon recovery, verify that the SMC may coordinate recovery from security events via electronic mail and the telephone. Upon completion of the User Registration and Accountability Audit Trail Reports at the sites, verify that the reports are sent to the SMC.

Check a new file into the CM tool. Verify that the Software Change Manager automatically creates and safeguards a file version whenever a new or changed file is checked into the library. Verify that the software library contains the master copy of all software that is deployed to the sites. Open a new CCR. Verify that upon completion of the change and closure of the CCR the new baseline record is sent to the SMC.

Test Outputs

Logs indicating invalid/valid logon attempts. Summary performance reports and notifications of performance metrics. Screen outputs notifying the user that they have entered an invalid username or password. Reports for user registration and accountability audit trails, a new software version and a CCR.

Success Criteria

This test will be deemed successful when all of the pre mentioned functionality has been verified and/or demonstrated.

Assumptions and Constraints

When a user logs in with an invalid ID the notification will not indicate whether the username or password was invalid.

4.15.11 Test Case 11: Data Access (BC031.009)

The purpose of Data Access Test is to test the functionality available for a user to update or modify the tables and fields in the database, load and transfer log files, schedule the archival of log files, transfer data from the DAACs to the SMC and read a selected record from the log file.

Test Inputs

Inputs to this test case include: selectively accessing the management data, updates to fields and tables, transferring and loading log files, archiving of log files and transferring of management data.

Test Steps

Using an application, access the management data.

Verify that the management data can be selectively accessed.

Using an application, update fields in the management database.

Using an application, test the ability to alter tables and fields in the database.

Demonstrate the capability to schedule the archiving of the log files at the site.

Demonstrate the capability of scheduling the transfer of management data from the sites to the SMC.

Verify that CSS sevices were utilized to access/transfer the management data.

Verify that records can be append to a log file using an application.

Using an application selectively read a record from a log file.

Verify that all of the above steps are executed while maintaining the integrity of the management database.

Test Outputs

Outputs to this test case include: selectivley accessing management data, accessed or transferred data via CSS services, a database with updated or altered fields, append and archived of log files and transfer of data occurring as scheduled, and a selected record.

Success Criteria

This test will be deemed successful when each of the above steps is tested or demonstrated to meet the desired criteria.

Assumptions and Constraints

None

4.15.12 Test Case 12: Office Automation (BC031.010)

The purpose of the Office Automation test is to demonstrate the desktop capabilities available in the Release A time frame.

Test Inputs

Inputs to this test include: inputs, transformations and editing of documents, insertion of worksheets and graphic images into documents, transfer and printing of documents, revisions to worksheets, developing of graphic images, insertion of the graphics image into a report.

Test Steps

Verify that the office automation tools to enable the generation of directives and instructions for recovery from detected security events are provided by the Security Management Application Service.

Initialize the word processor from the office automation work station.

Prepare, revise and record documents.

Import, transform and edit documents produced by other word processing packages.

Insert worksheets and graphic images into the document.

Transfer the document to spreadsheet and graphics applications.

Print the document.

Repeat appropriate steps for reports, data and messages.

Initialize the spreadsheet capabilities.

Demonstrate the systems availability to simulate and display an accountant's worksheet.

Demonstrate the capability to revise and perform calculations on the data.

Transfer the worksheet data to a word processing application (repeat for a graphics application).

Print the worksheet.

Initialize the graphics capabilities available through the office automation application.

Demonstrate the capability to develop, modify, record and print a graph.

Demonstrate the ability to transfer graphics images to word processing documents, messages, and reports.

Test Outputs

Outputs to this test case include: a document, report and message produced and revised by the office automation application, imported, transformed and edited documents produced by other word processing applications, worksheets and graphic images inserted into the document, an accountant's worksheet, revisions and calculations to the worksheet, a transfer of the worksheet to

a word file, a graph, modification, recording and printing to the graph and transfer of the graphs to another file.

Success Criteria

This test will be deemed successful when all of the document functionality available via the office automation application has been demonstrated.

Assumptions and Constraints

The office automation application is available and accessible.

4.15.13 Test Case 13: Report Generator (BC031.011)

The purpose of the Report Generator test case is to demonstrate/inspect all of the available functionality associated with the report generator. These tests will demonstrate the consistency between the functionality of the report generator and the level four requirements that were used to develop the design.

Test Inputs

Inputs to this test case include but are not limited to: all available reports, inputs to create ad hoc reports, management data maintained in the DBMS and the ability to redirect reports to a different device.

Test Steps

Verify that the report generator can receive information from the DBMS and generate reports from this information.

Demonstrate the existence of a Motif based Graphical User Interface (GUI) and the functionality associated with using the GUI to generate reports.

Demonstrate the ability of the report generator to generate ad hoc reports from the managed data maintained in the DBMS.

Verify that the reports generated can be formatted to contain any/all of the following information: title, header, footer, page number, date/time of report.

Demonstrate the capability to create charts and graphs from the management data contained in the DBMS.

Verify the ability of the report generator to redirect the output to the console, a disk file or a printer.

Test Outputs

Outputs to this test case include a variety of reports and charts directed to various output devices.

Success Criteria

This test will be deemed successful when the GUI is successfully used to generate a variety of reports based on the management data and these reports are capable of being output to a variety of different output devices.

Assumptions and Constraints

That there is data available in the DBMS.

5. CSMS Hardware/Performance Test Descriptions

The following sections identify the segment hardware and performance items used in CSMS for Release A. The hardware items have been grouped into easily testable configurations. Test cases to verify the functionality of the hardware items are documented. The general performance requirements (more specific performance requirements are covered throughout Section 4) are then identified and test cases to verify the performance issues are identified. The primary objective of each test case is to demonstrate and evaluate the capabilities of each function as stated in the Level 4 Requirements. All of these test cases will be performed at the Landover, Maryland EDF (see Section 3.3.4.1, Testing Facilities). Many of the test steps related to the hardware component inventory will be completed by EDS. The CSMS I&T staff will check off the requirement as being verified by EDS.

5.1 MSS Management Hardware CI Thread Test (TC032)

The MSS Management Hardware CI is the hardware to host all MSS software. This test will include the testing of the functional, performance, security and RMA requirements of the Enterprise Monitoring Server, Local Management Server, Management Workstations and Printers, which are the four logical components of MSS-MHCI.

5.1.1 Test Case 1: Enterprise Monitoring Server Test (TC032.001)

This test case verifies that the processors and the peripheral equipment provided by the Enterprise Monitoring Server meet the requirements established by the CSMS system design.

Test Inputs

Test Inputs include: an ingested fault to cause one of the servers to go down, update or fault at a DAAC, inspection and analysis of processes and procedures, peripherals, POSIX compliant vendor operating systems, inspection of data storage, upgrades to the disk drives, data, various tapes and a CD.

Test Steps

1. Inspect the Enterprise Monitoring Server and the Enterprise Communications Server and verify that they are physically and functionally identical. When one server goes down the other one provides backup service.
2. Verify that when updates occur at the Enterprise Monitoring Server or faults occur at a DAAC, the information is communicated between the Local System Management Server and the Enterprise Monitoring Server.
3. Analyze the functionality of the Enterprise Monitoring Server and verify that it does not interfere with operational processes during normal operations in the DAACs.
4. Inspect the Enterprise Monitoring Server and verify that the MSS software CIs are maintained by the server. Verify that the Management Workstations and Enterprise

Communications Server communicate along with the Enterprise Monitoring Server to create a local system management and coordination center for each ECS DAAC.

5. Verify that a dedicated terminal to be used as a local systems operations console is included in the Enterprise Monitoring Server processor.
6. Verify that the processor is expandable with additional quantities and types of peripherals and upgrade able/replaceable within the same product family without major software modifications or replacement of any attached component or peripheral.
7. Verify that the operating system is POSIX compliant IEEE 1003.1 and can support two dual-attached FDDI connections.
8. Install POSIX compliant operating systems from several vendors and verify that the Enterprise Monitoring Server short-term data storage is compatible with each one.
9. Verify that the Enterprise Monitoring Server intermediate-term data storage provides a minimum of 2.039 gigabytes and is upgradeable to 4.078 gigabytes.
10. Verify that the size and the data type of the Enterprise Monitoring Server intermediate-term data storage is compatible with the Local System Management Server short-term data storage.
11. Verify that the Enterprise Monitoring Server intermediate-term data storage supports RAID level 5: striping with interleaved parity. Also, verify that it contains the following hot swapple components: Disks, Power Supplies, Fans and Disk-array controllers.
12. Verify that the Enterprise Monitoring Server intermediate-term data storage and the Enterprise Communications Server intermediate-term data storage are the same storage connected to both servers and when one server goes down the other one provides the backup data.
13. Inspect the Enterprise Monitoring Server and verify that the intermediate-term data storage sustains 120 disk access/sec or better (4K block sizes) and the data in the storage can be archived and moved to the ECS data server archive for long-term storage.
14. Verify that the Enterprise Monitoring Server long-term data storage provides a minimum of 5.634 gigabytes and is upgradeable to 11.268 gigabytes. Also, verify that the data storage and retrieval meet ECS data server archival requirements.
15. Verify that the Enterprise Monitoring Server peripheral disk drives provide a minimum of 0.371 gigabytes and is upgradeable to 0.742 gigabytes.
16. Verify that data can be retrieved by the Enterprise Monitoring Server peripheral disk drives from both the Enterprise Monitoring Server short and long-term data storage.
17. Verify that one tape and one CD-ROM drive are supported by the Enterprise Monitoring Server peripherals.
18. Verify that the Enterprise Monitoring Server peripheral tape drive supports 4mm Digital Audio Tape format, accepts industry standard magnetic 4mm DAT (i.e. DDS-90), provides data transfer rate of 200KB/sec and is upgradeable/replaceable within the same product family.

19. Verify that the Enterprise Monitoring Server peripheral CD-ROM drive accepts 600MB Compact Disks and is upgradeable/replaceable within the same product family.
20. Verify that the Enterprise Monitoring Server maintains one backup of all software and key data items in a separate physical location and is capable of 100 percent growth in both processing speed and storage capacity without modifications or upgrades to software.
21. Verify that the hardware selection criteria of the Enterprise Monitoring Server meets the overall ECS security policies and system requirements.
22. Inspect the Enterprise Monitoring Server and the Local Management Server and verify that the MSS-MHCI functional string between the two servers provides a function Ao (operational availability) of 0.998 and an MDT of 20 minutes.

Test Outputs

A check list showing success or failure for each requirement.

Success Criteria

This test is successful when all the above requirements are met.

Assumptions and Constraints

The MSS Management Hardware CI is properly configured; Availability of the resources in the EDF.

5.1.2 Test Case 2: Local Management Server Test (TC032.002)

This test case verifies that the processors and the peripheral equipment provided by the Local Management Server meet the requirements established by the CSMS system design.

Test Inputs

Test Inputs include: an ingested fault to cause one of the servers to go down, update or fault at a DAAC, inspection and analysis of processes and procedures, peripherals, POSIX compliant vendor operating systems, inspection of data storage, upgrades to the disk drives, data, various tapes and a CD.

Test Steps

1. Inspect the Local Management Server and the Local Communications Server and verify that they are physically and functionally identical. When one server goes down the other one provides backup service.
2. Verify that when updates occur at the Enterprise Monitoring Server or faults occur at a DAAC, the information is communicated between the Local Management Server and the Enterprise Monitoring Server.
3. Analyze the functionality of the Local Management Server and verify that it only manages the local DAAC while preserving other DAAC autonomy of operations.

4. Inspect the Local Management Server and verify that the MSS software CIs are maintained by the server. Verify that the Management Workstations and Local Communications Server communicate along with the Local Management Server to create a local system management center for each ECS DAAC.

5. Verify that a dedicated terminal to be used as a local systems operations console is included in the Local Management Server processor.

6. Verify that the processor is expandable with additional quantities and types of peripherals and upgradeable/replaceable within the same product family without major software modifications or replacement of any attached component or peripheral.

7. Verify that the operating system is POSIX compliant IEEE 1003.1 and can support two dual-attached FDDI connections.

8. Install POSIX compliant operating systems from several vendors and verify that the Local Management Server short-term data storage is compatible with each one.

9. Verify that the Local Management Server short-term data storage provides a minimum of storage capacity (in gigabytes) for each DAAC configuration: 0.515 for GSFC LSM and EDC LSM, 0.459 for GSFC EOC, 0.505 for LaRC LSM and 0.472 for MSFC LSM. Also, verify that all these capacities are upgradeable to twice as much.

10. Verify that the size and the data type of the Local Management Server short-term data storage is compatible with the Enterprise Monitoring Server intermediate-term data storage.

11. Verify that the Local Management Server short-term data storage supports RAID level 5: striping with interleaved parity. Also, verify that it contains the following hot swapple components: Disks, Power Supplies, Fans, Disk-array controllers.

12. Verify that the Local Management Server and the Local Communications Server share the same short-term data storage. When one server goes down the other one provides the backup data.

13. Inspect the Local Management Server and verify that the short-term data storage sustain a disk access rate (per second) (4K block sizes) for each DAAC configuration: 48 or better for GSFC LSM and GSFC EOC, 51 or better for EDC LSM, 188 or better for LaRC LSM; 38 or better for MSFC LSM. Also, verify that the data in the storage can be archived and moved to the Enterprise Monitoring server intermediate-term data storage.

14. Verify that the Local Management Server peripheral disk drives provide a minimum of 0.371 gigabytes and is upgradeable to 0.742 gigabytes.

15. Verify that data can be retrieved by the Local Management Server peripheral disk drives from the Local Management Server short-term data storage.

16. Verify that one tape and one CD-ROM drive are supported by the Local Management Server peripherals.

17. Verify that the Local Management Server peripheral tape drive supports 4mm Digital Audio Tape format, accepts industry standard magnetic 4mm DAT (i.e. DDS-90), provides a data transfer rate of 200KB/sec and is upgradeable/replaceable within the same produce family.

18. Verify that the Local Management Server peripheral CD-ROM drive accepts 600MB Compact Disks and is upgradeable/replaceable within the same product family.
19. Verify that the Local Management Server maintains one backup of all software and key data items in a separate physical location and is capable of 100 percent growth in both processing speed and storage capacity without modifications or upgrades to software.
20. Verify that the hardware selection criteria of the Local Management Server meets the overall ECS security policies and system requirements.
21. Inspect the Enterprise Monitoring Server and the Local Management Server and verify that the MSS-MHCI functional string between the two servers provides a function Ao(operational availability) of 0.998 and an MDT of 20 minutes.
22. Verify that the MSS-MHCI functional string between the Local Management Server and ECS managed objects provides a function Ao of 0.998 and an MDT of 20 minutes.

Test Outputs

A check list showing success or failure for each requirement.

Success Criteria

This test is successful when all the above requirements are met.

Assumptions and Constraints

The MSS Management Hardware CI is properly configured. Availability of the resources in the EDF.

5.1.3 Test Case 3: Management Workstations and Printers Test (TC032.003)

This test case verifies that the processors and the peripheral equipment provided by the Management Workstations and all the Printers meet the requirements established by the CSMS system design.

Test Inputs

Startup and shutdown of various workstations and servers, policies and procedures, and hardware associated with the workstations and printers.

Test Steps

1. Turn on several Management Workstations and processors and verify that they operate simultaneously without interfering with each other, when some workstations or management/communications servers go down, the operations at the other Management Workstations and processors are not affected.
2. Verify that the operating system is POSIX compliant IEEE 1003.1 and can support AUI 802.3 Ethernet connection and provide 46 Mbyte of internal RAM.

3. Verify that one QWERTY keyboard which is detachable and cabled for movement on a desk-top style workstation area and provides a minimum of 12 programmable function keys is provided by each Management Workstation.
4. Verify that one color text and graphics display device with the following features is provided by each Management Workstation. Display the complete ASCII character set, a minimum of 16 colors and 4 screen display pages, pages 24 lines by 80 characters wide which are readable from any location along the width of the workstation and up to a distance of 6 feet from the screen. Provide a minimum of 1024 pixel x 864 lines resolution display, 19 inch diagonal non-glare screen, RGB video output for hard copy and brightness, contrast and power controls within easy reach; Feature an integral swivel/tilt base. Be physically relocatable within the operations center.
5. Verify that each Management Workstation provides one cursor pointing device (mouse) and upgradeable/replaceable within the same product family.
6. Verify that The Management Workstation data storage is capable of retrieving data from the data storage function of both the Enterprise Monitoring Server and the Local Management Server.
7. Verify that the Management Workstation disk drives provide a minimum of 0.296 gigabytes and are upgradeable to 0.591 gigabytes. Also, verify that all the disk drives serving a specific function (e.g., local management, enterprise monitoring) are identical with equal capacity.
8. Inspect all the shared system printers attached to the network and verify that they are physically and functionally identical.
9. Verify that the hardware selection criteria of the Management Workstations and Printers meets the overall ECS security policies and system requirements.

Test Outputs

A check list showing success or failure for each requirement.

Success Criteria

This test is successful when all the above requirements are met.

Assumptions and Constraints

The MSS Management Hardware CI is properly configured. Availability of the resources in the EDF.

5.2 CSS Distributed Communications Hardware CI Thread Test (TC033)

The CSS Distributed Communications Hardware CI (CSS-DCHCI) is the hardware to host all CSS software. This test will include the testing of the functional, security and RMA requirements of the Enterprise Communications Server, Local Communications Server, and the Bulletin Board Server, which are the three logical components of MSS-MHCI.

5.2.1 Test Case 1: Enterprise Communications Server Test (TC033.001)

This test case verifies that the processors and the peripheral equipment provided by the Enterprise Communications Server meet all the requirements established by the CSMS system design.

Test Inputs

Test Inputs include: an ingested fault to cause one of the servers to go down, update or fault at a DAAC, inspection and analysis of processes and procedures, peripherals, POSIX compliant vendor operating systems, inspection of data storage, upgrades to the disk drives, data, various tapes and a CD.

Test Steps

1. Inspect the Enterprise Monitoring Server and the Enterprise Communications Server and verify that they are physically and functionally identical. When one server goes down the other one provides backup service.
2. Verify that when updates occur at the Enterprise Communications Server or faults occur at a DAAC, the information is communicated between the Local Communications Servers and the Enterprise Communications Server.
3. Analyze the functionality of the Enterprise Communications Server and verify that it does not interfere with operational processes during normal operations in the DAACs.
4. Inspect the Enterprise Communications Server and verify that the CSS software CIs are maintained by the server. Verify that the Management Workstations and Enterprise Monitoring Server communicate along with the Enterprise Communications Server to create an enterprise management and coordination center for the ECS.
5. Verify that a dedicated terminal to be used as a local systems operations console is included in the Enterprise Communications Server processor.
6. Verify that the processor is expandable with additional quantities and types of peripherals and upgradeable/replaceable within the same product family without major software modifications or replacement of any attached component or peripheral.
7. Verify that the operating system is POSIX compliant IEEE 1003.1 and can support two dual-attached FDDI connections.
8. Install POSIX compliant operating systems from several vendors and verify that the Enterprise Communications Server intermediate-term data storage is compatible with each one.
9. Verify that the Enterprise Communications Server intermediate-term data storage provides a minimum of 2.039 gigabytes and is upgradeable to 4.078 gigabytes.
10. Verify that the size and the data type of the Enterprise Communications Server intermediate-term data storage is compatible with the Local Communications Server short-term data storage.

11. Verify that the Enterprise Communications Server intermediate-term data storage supports RAID level 5: striping with interleaved parity. Also, verify that it contains the following hot swapple components: Disks, Power Supplies, Fans, Disk-array controllers.

12. Verify that the Enterprise Communications Server and the Enterprise Monitoring Server share the same intermediate-term data storage. When one server goes down the other one provides the backup data.

13. Inspect the Enterprise Communications Server and verify that the intermediate-term data storage sustains 120 disk access/sec or better (4K block sizes) and the data in the storage can be archived and moved to the ECS data server archive for long-term storage.

14. Verify that the Enterprise Communications Server long-term data storage provides a minimum of 5.634 gigabytes and is upgradeable to 11.268 gigabytes. Also, verify that the data storage and retrieval meet ECS data server archival requirements.

15. Verify that the Enterprise Communications Server peripheral disk drives provide a minimum of 0.371 gigabytes and is upgradeable to 0.742 gigabytes.

16. Verify that data can be retrieved by Enterprise Communications Server peripheral disk drives from both the Enterprise Communications Server short and long-term data storage.

17. Verify that one tape and one CD-ROM drive are supported by the Enterprise Communications Server peripherals.

18. Verify that the Enterprise Communications Server peripheral tape drive supports 4mm Digital Audio Tape format, accepts industry standard magnetic 4mm DAT(i.e. DDS-90), provides data transfer rate of 200KB/sec and is upgradeable/replaceable within the same product family.

19. Verify that the Enterprise Communications Server peripheral CD-ROM drive accepts 600MB Compact Disks and is upgradeable/replaceable within the same product family.

20. Verify that the Enterprise Communications Server time source is a GFE NASA-36 bit serial time code signal synchronized to GMT.

21. Verify that the Enterprise Communications Server time source provides the master source to software-based time services throughout the ECS.

22. Verify that the hardware selection criteria of the Enterprise Communications Server meets the overall ECS security policies and system requirements.

23. Analyze the Enterprise Communications Server and verify that it is configured to provide autonomous DAAC security perimeter and an ISO CELL ECS security perimeter.

24. Verify that the Enterprise Communications Server maintains one backup of all software and key data items in a separate physical location.

25. Inspect the Enterprise Communications Server and the Local Communications Server and verify that the MSS-MHCI functional string between the two server provides a function Ao of 0.96 (0.998 design goal) and an MDT of four hours (1.5 hour design goal).

26. Verify that the CSS-DCHCI Enterprise Communications Server provides a function Ao of 0.998 (0.999998 design goal) and an MDT of 20 minutes (design goal of 5 minutes) for all functions integral to providing a backup to the Enterprise Monitoring Server . Also, verify that for those functions not integral to providing backup functionality to the Enterprise Monitoring Server, the function Ao is 0.96 (0.998 design goal) and MDT is four hours (1.5 hour design goal).

Test Outputs

A check list showing success or failure for each requirement.

Success Criteria

This test is successful when all the above requirements are met.

Assumptions and Constraints

The CSS Distributed Communications Hardware CI is properly configured. Availability of the resources in the EDF.

5.2.2 Test Case 2: Local Communications Server Test (TC033.002)

This test case verifies that the processors and the peripheral equipment provided by the Local Communications Server meet all the requirements established by the CSMS system design.

Test Inputs

Test Inputs include: an ingested fault to cause one of the servers to go down, update or fault at a DAAC, inspection and analysis of processes and procedures, peripherals, POSIX compliant vendor operating systems, inspection of data storage, upgrades to the disk drives, data, various tapes and a CD.

Test Steps

1. Inspect the Local Management Server and the Local Communications Server and verify that they are physically and functionally identical. When one server goes down the other one provides the backup service.
2. Verify that when updates occur at the Enterprise Communications Server or faults occur at a DAAC, the information is communicated between the Local Communications Servers and the Enterprise Communications Server.
3. Analyze the functionality of the Local Communications Server and Verify that it is configurable according to local DAAC user authentication/authorization policy and does not interfere with operational processes during normal operations in other DAACs.
4. Inspect the Local Communications Server and verify that the CSS software CIs are maintained by the server. Verify that the Management Workstations and Local Management Server communicate along with the Local Communications Server to create a local system management center for each ECS DAAC.

5. Verify that a dedicated terminal to be used as a local systems operations console is included within the Local Communications Server processor.

6. Verify that the processor is expandable with additional quantities and types of peripherals and upgradeable/replaceable within the same product family without major software modifications or replacement of any attached component or peripheral.

7. Verify that the operating system is POSIX compliant IEEE 1003.1 and can support two dual-attached FDDI connections.

8. Install POSIX compliant operating systems from several vendors and verify that the Local Communications Server short-term data storage is compatible with each one.

9. Verify that the Local Communications Server short-term data storage provides a minimum of storage capacity (in gigabytes) for each DAAC configuration: 0.515 for GSFC LSM and EDC LSM; 0.459 for GSFC EOC; 0.505 for LaRC LSM; 0.472 for MSFC LSM. Also, verify that all these capacities are upgradeable to twice as much.

10. Verify that the size and the data type of the Local Communications Server short-term data storage is compatible with the Enterprise Communications Server intermediate-term data storage.

11. Verify that the Local Communications Server short-term data storage supports RAID level 5: striping with interleaved parity. Also, verify that it contains the following hot swappable components: Disks, Power Supplies, Fans, Disk-array controllers.

12. Verify that the Local Communications Server and the Local Management Server share the same short-term data storage. When one server goes down the other one provides the backup data.

13. Inspect the Local Communications Server and verify that the short-term data storage sustains a disk access rate (per second) (4K block sizes) for each DAAC configuration: 48 or better for GSFC LSM and GSFC EOC; 51 or better for EDC LSM; 188 or better for LaRC LSM; 38 or better for MSFC LSM. Also, verify that the data in the storage can be archived and moved to the Enterprise Communications server intermediate-term data storage.

14. Verify that the Local Communications Server peripheral disk drives provide a minimum of 0.371 gigabytes and is upgradeable to 0.742 gigabytes.

15. Verify that data can be retrieved by Local Communications Server peripheral disk drives from both the Local Communications Server short-term and long-term data storage.

16. Verify that one tape and one CD-ROM drive are supported by the Local Communications Server peripherals.

17. Verify that the Local Communications Server peripheral tape drive supports 4mm Digital Audio Tape format, accepts industry standard magnetic 4mm DAT(i.e. DDS-90), provides data transfer rate of 200KB/sec and is upgradeable/replaceable within the same product family.

18. Verify that the Local Communications Server peripheral CD-ROM drive accepts 600MB Compact Disks and is upgradeable/replaceable within the same product family.
19. Change the time source in the Enterprise Communications Server and verify that the Local Communications Server time source changes accordingly for software-based time services throughout the ECS.
20. Verify that the hardware selection criteria of the Local Communications Server meets the overall ECS security policies and system requirements.
21. Analyze the Local Communications Server and verify that it is configured to provide autonomous DAAC security perimeter, FOS isolation, and an ISO CELL ECS security perimeter.
22. Verify that the local Communications Server maintains one backup of all software and key data items in a separate physical location.
23. Inspect the Enterprise Communications Server and the Local Communications Server and verify that the MSS-MHCI functional string between the two server provides a function Ao of 0.96 (0.998 design goal) and an MDT of four hours (1.5 hour design goal).
24. Verify that the CSS-DCHCI functional string between the Local Communications Server and ECS clients to the Server provides a function Ao of 0.96 (0.998 design goal) and an MDT of four hours (1.5 hour design goal).
25. Verify that the Local Communications Server provides a function Ao of 0.998 (0.999998 design goal) and an MDT of 20 minutes (design goal of 5 minutes) for all functions integral to providing a backup to the Local Management Server . Also, verify that for those functions not integral to providing backup functionality to the Local Management Server, the function Ao is 0.96 (0.998 design goal) and MDT is four hours (1.5 hour design goal).

Test Outputs

A check list showing success or failure for each requirement.

Success Criteria

This test is successful when all the above requirements are met.

Assumptions and Constraints

The CSS Management Hardware CI is properly configured. Availability of the resources in the EDF.

5.2.3 Test Case 3: Bulletin Board Server Test (TC033.003)

This test case verifies that the processors and the peripheral equipment provided by the Bulletin Board Server meet the requirements established by the CSMS system design.

Test Inputs

Shared data between Bulletin Board Server and Enterprise Communications Server, policies and procedures relating to the Bulletin Board Server, Contents of Bulletin Board Server, POSIX

compliant vendor specific operating systems, various tapes, a CD, a new time source and security policies and procedures.

Test Steps

1. Inspect the Bulletin Board Server and verify that it shares data with the Enterprise Communications Server to prevent a single point of failure for user community access to directory data.
2. Analyze the Bulletin Board Server and verify that it is configurable according to local DAAC user authentication/authorization policy, it does not interfere with operational processes during normal operations in other DAACs, but yet is able to provide a integrated view of ECS for user registration, account administration and authentication/authorization to ECS services.
3. Inspect the Bulletin Board Server and verify that the CSS software CIs are maintained by the server to create a single, secure unified access to all ECS services. Also, verify that ECS client software and toolkits are located in the server for ECS-external distribution.
4. Verify that a dedicated terminal to be used as a local systems operations console is included within the Bulletin Board Server processor.
5. Verify that the processor is expandable with additional quantities and types of peripherals and upgradeable/replaceable within the same product family without need for any perturbation of any software modifications or replacement of any attached component or peripheral.
6. Verify that the operating system is POSIX compliant IEEE 1003.1 and can support two dual-attached FDDI connections.
7. Install POSIX compliant operating systems from several vendors and verify that the Bulletin Board Server intermediate-term data storage is compatible with each one.
8. Verify that the Bulletin Board Server intermediate-term data storage provides a minimum storage capacity of 1.189 gigabytes and upgradeable to 2.378 gigabytes. Also, verify that data in the Bulletin Board Server intermediate-term storage can be archived and sent to the ECS data server archive for long-term storage and software/toolkit safestore.
9. Verify that the Bulletin Board Server long-term data storage provides a minimum storage capacity of 3 gigabytes and upgradeable to 6 gigabytes and data storage and retrieval meet the ECS data server archival requirements.
10. Verify that one tape and one CD-ROM drive are supported by the Bulletin Board Server peripherals.
11. Verify that the Bulletin Board Server peripheral tape drive supports 4mm Digital Audio Tape format, accepts industry standard magnetic 4mm DAT(i.e. DDS-90), provides a data transfer rate of 200KB/sec and is upgradeable/replaceable within the same produce family.
12. Verify that the Bulletin Board Server peripheral CD-ROM drive accepts 600MB Compact Disks and is upgradeable/replaceable within the same product family.

13. Change the time source in the Enterprise Communications Server and verify that the Bulletin Board Server time source changes accordingly for software-based time services throughout the ECS.
14. Verify that the hardware selection criteria of the Bulletin Board Server meets the overall ECS security policies and system requirements.
15. Verify that the CSS-DCHCI Bulletin Board Server provides a security perimeter for ECS and a function Ao of 0.96 (0.998 design goal) and an MDT of four hours (1.5 hour design goal).

Test Outputs

A check list showing success or failure for each requirement.

Success Criteria

This test is successful when all the above requirements are met.

Assumptions and Constraints

The CSS Management Hardware CI is properly configured. Availability of the resources in the EDF.

5.3 ISS Internetworking Hardware CI Thread Test (TC034)

The ISS Internetworking Hardware CI (ISS-INHCI) is the hardware to host all ISS software. This test will include the testing of the functional, performance, security and evolvability requirements of the ISS-INHCI.

5.3.1 Test Case 1: ISS-INHCI Functional Requirements Test (TC034.001)

This test case verifies all the functional requirements of ISS Release A LANs, ISS Components and LAN Analysis Equipment .

Test Inputs

Policies, procedures, and hardware.

Test Steps

1. Verify that LANs are provided by ISS at the following Release A sites: GSFC DAAC, GSFC EOC, EDC DAAC, LaRC DAAC AND MSFC DAAC.
2. Verify that all the physical devices and Medium Access Control protocols used in ISS are compatible with IEEE 80.2 (Logical Link Control), 80.3 (MAC for Ethernet), 80.6 (MAC for SMDS) and ANSI X3T9.5 (MAC for FDDI).
3. Verify that all the physical components and services in ISS can be monitored via SNMP agents.

4. Verify that the LAN Analysis Equipment provides protocol analysis through the transport layer for all ISS LAN protocols and interconnection protocols to MANs/WANs.
5. Verify that the LAN Analysis Equipment includes one LAN analyzer, one digital VOM/multimeter and one communications line monitor to store and display up to 10,000 bytes of data sent and received over any of the communications lines at rates of 10MB/sec to 100 MB/sec, and supporting the protocols used within and interconnecting ECS.

Test Outputs

A check list showing success or failure for each requirement.

Success Criteria

This test is successful when all the above requirements are met.

Assumptions and Constraints

The ISS Internetworking Hardware CI is properly configured. Availability of the resources in the EDF.

5.3.2 Test Case 2: ISS-INHCI Performance Requirements Test (TC034.002)

This test case verifies all the performance requirements of the ISS-INHCI.

Test Inputs

Drivers to initialize and load the EOC LAN loop delay, network devices, various data rates and traffic rates, drivers to load the drive the bandwidth and simulated network traffic loads.

Test Steps

1. Verify that the EOC LAN loop delay contribution does not exceed more than the expected (goal 250 msec) seconds of the total ECS delay of 2.5 seconds for emergency real-time commands.
2. Verify that the EOC Operational LAN is able to support 230 network devices and peak data rates of up to 48 Mbps without redesign and its backbone is able to support a peak traffic rate of 24 Mbps to support AM-1 flows from the Ecom interface.
3. Verify that ISS provides wide area bandwidth necessary to support data transfer in accordance with Release A requirements specified in "Communications Requirements for the ECS Project", 194-220-SE3-001
4. Verify that the ISS provides sufficient [the specified amount will be tested] local area network bandwidth at the LaRC, MSFC, GSFC and EDC DAACs to support data transfer between and among physical nodes provided by SDPS, MSS and CSS for Release A.
5. Verify that the ISS LANs at the GSFC, MSFC and LaRC DAAC sites are capable of supporting network traffic load estimates [the specified amount will be tested] without redesign through Release B and ISS LANs at the Release-A DAAC sites are designed to

allow nodes to be added to any given LAN segment and additional LAN segments to be added to the LAN.

Test Outputs

A check list showing success or failure for each requirement.

Success Criteria

This test is successful when all the above requirements are met.

Assumptions and Constraints

The ISS Internetworking Hardware CI is properly configured. Availability of the resources in the EDF.

5.3.3 Test Case 3: ISS-INHCI Security and Evolvability Requirements Test (TC034.003)

This test case verifies all the security and evolvability requirements of the ISS-INHCI.

Test Inputs

Drivers to simulate the access of network and transport layer filtering from internal and external interfaces. Expanding of the networks and increased data volumes.

Test Steps

1. Verify that the ISS network supports the use of network and transport layer filtering to control access from internal and external interfaces.
2. Verify that the ISS-IBHCI DAAC LANs provide transparent portability across heterogeneous site LAN architectures and enables expansion to GByte networks including the ability to provide increased volume of data distribution and access.

Test Outputs

A check list showing success or failure for each requirement.

Success Criteria

This test is successful when all the above requirements are met.

Assumptions and Constraints

The ISS Internetworking Hardware CI is properly configured. Availability of the resources in the EDF.

5.4 Facility Requirements Thread Test (TC035)

This test will include the following three sections: EMC Test, LSM test and Infrastructure Test.

5.4.1 Test Case 1: EMC Test (TC035.001)

DAAC	Requirements	Inspected
EDF	In the IR-1 timeframe:	
	1. Provide a Enterprise Monitoring Server configured with: two fixed disks, one tape drive, one CD-ROM drive and storage cross-strapped with Enterprise Communications Server.	
	2. Provide a Enterprise Communication Server configured with: two fixed disks, one tape drive, one CD-ROM drive, one slaved time source and storage cross-strapped with Enterprise Monitoring Server.	
	3. Provide a Bulletin Board Server configured with: one tape drive, one CD-ROM drive and one fixed drive	
	4. Provide two intermediate-term Data Storage Unit supporting RAID level 5, one for the shared Enterprise Monitoring/Enterprise Communications, and the other for the Bulletin Board Server.	
	5. Provide one system printer and two Management Workstations, which can perform any EMC Function	
GSFC	In the R-A timeframe:	
	1. Provide an Enterprise Monitoring Server, an Enterprise Communications Server and a Bulletin Board Server transferred from the IR-1 EDF.	
	2. Provide an Enterprise Monitoring Server long-term data storage capability via the ECS data server.	

5.4.2 Test Case 2: LSM Test (TC035.002)

DAAC	Requirements	Inspected		
GSFC	In the IR-1 time frame, All these DAACs should provide a local Management Server configured with: two fixed disks, one tape drive and one CD-ROM drive.			
MSFC				
LaRC				
EDC				
GSFC	In the R-A timeframe, All these DAACs should provide 1. a Local Communications Server configured with :			
EOC	two fixed disks, one tape drive, one CD-ROM drive , one slaved time source and storage cross-strapped with Local			
MSFC	Management Server. 2. one short-term data storage unit supporting RAID level 5			
LaRC	cross strapped between the local management and communications servers.			
EDC	3. one system printer and two management workstations which can perform any EOC LSM function			
EOC	In the IR-1 time frame, provide a Local Management Server configured with: two fixed disks, one tape drive, one CD-ROM drive and storage cross-strapped with Local Communications Server.			

5.4.3 Test Case 3: Infrastructure Test (TC035.003)

DAAC	Requirements	Inspected
EDF	Provide one EDF LAN in the IR-1 timeframe	
GSFC	Provide one GSFC LAN in the IR-1 timeframe	
EOC	Provide one EOC LAN in the IR-1 timeframe	
MSFC	Provide one MSFC LAN in the IR-1 timeframe	
LaRC	Provide one LaRC LAN in the IR-1 timeframe	
EDC	Provide one EDC LAN in the IR-1 timeframe	

5.5 Performance Testing (TC036)

This test will cover the performance issues related to the CSS and MSS services.

The object of this test is to verify that the resources required to meet the performance standards set forth in the CSMS Level 4 Requirements are obtainable.

Special resources required for this build test include:

- XRunner
- LoadRunner
- HP OpenView Network Framework
- Network Analyzer

There is one performance management test case in this section:

5.5.1 Test Case 1: Performance Management (TC036.001)

This test case tests the performance issues related to the resources provided to the DAACs.

Test Inputs

XRunner and LoadRunner scripts to simulate multiple users performing multiple tasks with the purpose of loading the system resources.

Simulated IV&V activities.

Configuration data and database activity.

Test Steps

Simulate as much activity as possible over the network and various tasks taking place.

Verify that at a critical point the MDT is 20 minutes or less for critical services and runs at an operational availability of .998 at a minimum for the CSS services (repeat for MSS services).

Verify that at all times CSS services allocate atleast 10% of the development resources for IV&V activities. (repeat for MSS services)

Attempt to disrupt the activities associated with the network databases and configuration data.

Verify that the CSS services contains no single point of failure. (repeat for MSS services)

Test Outputs

Outputs to this test case will be the availability of the necessary resources.

Success Criteria

The following test will be successful when all of the resources have been "pushed to the limit" and the above thresholds are still obtained.

Assumptions and Constraints

Using XRunner and LoadRunner we will be able to simulate a load over on the network.

Appendix A. Test Tool Descriptions

The following matrix gives a listing and description of available test tools.

TOOL TYPE	SELECTED TOOL	TOOL DESCRIPTION
Configuration Management Tool	ClearCase	Developed by Atria Software, Inc. Uses VOBs (Version Object Base) to store the software versions. A VOB is a virtual directory tree of sources and other objects and is mounted like a disk partition. A project may have many VOBs. Any changes made by the developer after the software has been frozen will be conducted on a branch. The test organizations are responsible for merging the fixes (branches).
Non Conformance Reporting Tool	DDTS	Distributed Defect Tracking System (DDTS) developed by QualTrak Corporation. DDTS is a UNIX change management and bug tracking system that tracks and manages changes throughout the life cycle of a hardware or software product from initial requirements planning to obsolescence in the field. DDTS was specifically designed to aid developers during product development and the quality assurance organization during the testing phase. This tool works hand and hand with ClearCase.
Capture and Playback Tool	XRunner	XRunner was developed by Mercury Interactive Corporation. XRunner is an advanced automated software testing system for X window applications. XRunner automates the full range of software testing needs. Some of the gained functionality include: output synchronization, text recognition and a high-level testing mode that operates directly on GUI objects.
Automated Client/Server Testing System	LoadRunner	LoadRunner was developed by Mercury Interactive Corporation. It is an automated testing system for client/server applications on UNIX/X platforms. By running multiple users in parallel off the server, LoadRunner enables us to automate load testing, performance testing, and system tuning.
Requirements Traceability Tool	RTM	Requirements & Traceability Management tool is developed by GEC-Marconi Limited configurable to support our methodology. RTM provides an audit trail that will enable us to trace various requirements. The tool is driven by requirements and provides an easy avenue for the production of requirements related documents or matrix.
Network Management Framework	OpenView	OpenView was developed by Hewlett Packard. It is a Network Management Framework. The Framework can be used to monitor any device that supports the Simple Network Management Protocol (SNMP). This tool will aid us in determining the status of the network and devices on the network.
OOA/OOD Tool	StP / OMT	Use of the following graphs and charts for the future development of test procedures:State Transition Diagrams (STDs) Event Trace Diagrams Data Flow Diagrams (DFDs) Data Dictionaries Decision Tables Process Activation Tables and others.

This page intentionally left blank.

Appendix B. Verification Traceability Matrix

The following matrix provides a mapping of Level 4 requirements to Build/Test case.

req_source_id	text	csci_id	release	Case /thread	verification
C-CSS-00010	The CSS services shall have an operational availability of .998 at a minimum and an MDT of 20 minutes or less for critical services.	DCCI	A	TC036.001	verification
C-CSS-00020	The CSS services shall have no single point of failure for functions associated with network databases and configuration data.	DCCI	A	TC036.001	Test
C-CSS-00030	The CSS services shall be extensible in its design to provide capability for growth and enhancement.	DCCI	A	BC012.001	Test
C-CSS-00100	The CSS Directory service shall maintain multiple copies of the namespace on different hosts to provide fault tolerance.	DCCI	A	TC019.001	Test
C-CSS-00200	The CSS services shall allocate 10% of development resources for IV&V activity.	DCCI	A	TC036.001	Inspec.
C-CSS-01000	The CSS DOF Service shall provide a standards-based Interface Definition Language (IDL) and language mappings to at least C and C++ (limited) languages.	DCCI	A	TC023.004	Inspec.
C-CSS-01010	The CSS DOF provided IDL shall support versioning of the interface supporting minor and major versions.	DCCI	A	TC023.004	Inspec.
C-CSS-01020	The IDL supported minor versioning shall be upward compatible that requires no changes in the client software to communicate with the new implementation.	DCCI	A	TC023.004	Demo Inspec.

C-CSS-01030	The CSS DOF Service shall support the passing of the general error status as a parameter in calls between the clients and servers automatically.	DCCI	A	TC023.004	Demo
C-CSS-01040	The CSS DOF Service shall provide the capability to marshal and unmarshal the arguments and the returned value transparently while making a remote procedure call.	DCCI	A	TC023.004	Demo
C-CSS-01050	The CSS DOF Service shall provide the capability to marshal and unmarshal standard types to/from a common standard format.	DCCI	A	TC023.004	Demo
C-CSS-01060	The CSS DOF Service shall provide the capability to define marshaling and unmarshaling routines for user defined types.	DCCI	A	TC023.004	Demo
C-CSS-01070	The CSS DOF Service shall provide server APIs to register/unregister services in the namespaces (in different administrative domains) under different views (server/group/profile).	DCCI	A	TC023.005	Demo
C-CSS-01080	The CSS DOF Service shall provide server APIs to register/unregister different implementations of an interface in the namespace.	DCCI	A	TC023.005	Test
C-CSS-01090	The CSS DOF Service shall provide server APIs to register/unregister individual objects implementing an interface in the namespace.	DCCI	A	TC023.005	Test
C-CSS-01100	The CSS DOF Service shall provide server APIs to register their services using different protocols in the namespace.	DCCI	A	TC023.005	Test
C-CSS-01110	The CSS DOF Service shall provide server APIs to register their services with the local endpoint mapper with the proper port number.	DCCI	A	TC023.005	Test

C-CSS-01120	The CSS DOF Service shall provide mechanisms to shutdown a service gracefully, by allowing the servers to unregister the server information from the namespace.	DCCI	A	TC023.004	Test
C-CSS-01130	The CSS DOF Service shall provide server APIs to limit the maximum number of threads to use in servicing the requests concurrently.	DCCI	A	TC023.005	Demo
C-CSS-01140	The CSS DOF Service shall provide client APIs to bind to services (registered in the local namespace as well as remote namespaces) by using any of the following information to achieve location transparency of services. a._a service name b._an interface name c._an object name d._a host name and communication protocol e._an object reference	DCCI	A	TC023.005	Test
C-CSS-01150	The CSS DOF Service shall return gracefully by throwing an exception or returning an error code when it can not retrieve the binding information or can not resolve a binding.	DCCI	A	TC023.004	Test
C-CSS-01160	The CSS DOF Service shall provide client APIs to specify a confidence level of the binding information as follows: a._a low confidence level indicating the use of a local cache to obtain binding information b._a medium confidence level indicating the DOF to get the binding information from any of the directory replicas. c._a high confidence level indicating the DOF to get the binding information from the master copy of the directory services.	DCCI	A	TC023.005	Demo

C-CSS-01170	The CSS DOF Service shall provide APIs to set/get the authentication service type to be used between the server and the client.	DCCI	A	TC023.005	Test
C-CSS-01180	The CSS DOF Service shall provide APIs to set/get authorization service type to be used between the client and tha server.	DCCI	A	TC023.005	Test
C-CSS-01190	The CSS DOF Service shall provide APIs to maintain the integrity of the data to be passed between the client and the server.	DCCI	A	TC023.005	Test
C-CSS-01200	The CSS DOF Service shall provide APIs to maintain the privacy of the data passed between the client and the server by encrypting and decrypting the data.	DCCI	A	TC023.005	Test
C-CSS-01210	The CSS DOF Service shall provide APIs to set the identity of a given principal to a given process.	DCCI	A	TC023.005	Test
C-CSS-01220	The CSS DOF shall support the TCP and UDP communication protocols to communicate between the servers and the clients.	DCCI	A	TC023.004	Test
C-CSS-10100	The CSS shall interface with the SDPS subsystems to exchange the data items in Table 6-1 as specified in the ECS internal ICDs, 313-DV3-003.	DCCI	A	BC023.007	Demo
C-CSS-10200	The CSS shall interface with the FOS subsystems to exchange the data items in Table 6-2 as specified in the ECS internal ICDs, 313-DV3-003.	DCCI	A	BC023.007	Test
C-CSS-10300	The CSS shall interface with the MSS subsystems to exchange the data items in Table 6-3 as specified in the ECS internal ICDs, 313-DV3-003.	DCCI	A	BC031.013	Test

C-CSS-10400	The CSS shall interface with the ISS subsystems to exchange the data items in Table 6-4 as specified in the ECS internal ICDs, 313-DV3-003.	DCCI	A	BC023.007	Test
C-CSS-20000	The CSS Directory service shall provide the basic functionality to save and retrieve information into the local namespace: a._Create/Delete/Get context (key) b._List context. c._Set/Get attributes. d._Create/Delete attributes. e._List attributes. f._Set/Get attribute information.	DCCI	A	TC019.001	Test
C-CSS-20010	The CSS Directory Service shall provide implementations of the DNS and X.500 namespaces.	DCCI	A	TC019.001	Demo
C-CSS-20020	The CSS Directory service shall provide a mechanism to periodically update copies of the namespace from the namespace designated as the master.	DCCI	A	TC019.001	Demo Inspection
C-CSS-20025	The updating of the namespace shall be done a._automatically b._manually by the administrator.	DCCI	A	TC019.001	Demo
C-CSS-20030	The CSS Directory Service shall provide the capability to partition the namespace and distribute and maintain them at different hosts on the network.	DCCI	A	TC019.001	Demo
C-CSS-20040	The CSS Directory Service shall provide the capability to replicate partitions of the namespace on different hosts.	DCCI	A	TC019.001	Demo
C-CSS-20050	The CSS Directory service shall provide multiple directory agents which cooperate among themselves through referral and chaining to perform directory operations.	DCCI	A	TC019.003	Demo
C-CSS-20060	The CSS Directory service shall provide a way to denote the relative root of the namespace.	DCCI	A	TC019.001	Demo

C-CSS-20070	The CSS Directory Service shall maintain local cache to keep recently lookup information from the namespace for more efficient further lookups.	DCCI	A	TC019.001	Demo Inspection
C-CSS-20080	The CSS Directory Service shall interact with the Security Service to provide host based security to the entries in the namespace.	DCCI	A	TC019.001	Demo Inspection
C-CSS-20090	The CSS Directory service shall define a minimum of 20 user defined attribute types for application users to store/retrieve attribute information.	DCCI	A	TC019.002	Test
C-CSS-20110	The CSS Directory service shall determine which naming service to use from a given context.	DCCI	A	TC019.002	Demo Inspection
C-CSS-20120	The CSS Directory service shall provide a mechanism to communicate with both X.500 and DNS naming services in resolving lookups.	DCCI	A	TC019.003	Demo
C-CSS-21000	The CSS Security service shall provide an API to verify the identity of users.	DCCI	A	TC024.001	Demo Inspection
C-CSS-21020	The CSS Security service shall provide the capability to create/modify/delete user accounts and privileges in the security registry.	DCCI	A	TC024.005	Test
C-CSS-21030	The CSS Security service shall provide the capability to define/modify/delete group information in the security registry.	DCCI	A	TC024.005	Demo
C-CSS-21040	The CSS Security service shall provide an API to limit the time after which a login context will expire.	DCCI	A	TC024.003	Demo
C-CSS-21050	The CSS Security Service shall provide an API to refresh login contexts before they expire.	DCCI	A	TC024.003	Test
C-CSS-21060	The CSS Security Service shall provide an API to accept server keys associated with services interactively at the startup of a service.	DCCI	A	TC024.002	Test

C-CSS-21070	The CSS Security Service shall provide an API to store server keys associated with servers to a disk file.	DCCI	A	TC024.002	Test
C-CSS-21080	The CSS Security Service shall provide an API to retrieve the server keys associated with services from a disk file at startup time to authenticate the service.	DCCI	A	TC024.002	Test
C-CSS-21090	The CSS Security Service shall provide an API to change the identity of an application process through server keys.	DCCI	A	TC024.002	Test
C-CSS-21100	The CSS Security service shall provide an API to challenge the client/server to authenticate itself at the following three levels. a._connect level b._request level c._packet level	DCCI	A	TC024.002	Test
C-CSS-21110	The CSS Security service shall authenticate the principal before checking whether the principal is authorized to access a service.	DCCI	A	TC024.005	Test
C-CSS-21120	The CSS Security service shall provide an API to check the authorization privileges of principals to access/control resources.	DCCI	A	TC024.005	Test
C-CSS-21130	The CSS Security Service shall provide an API to define the permission schema associated with a server.	DCCI	A	TC024.005	Test
C-CSS-21140	The CSS Security Service shall provide an API to create and maintain the ACLs associated with the server in a database.	DCCI	A	TC024.004	Test
C-CSS-21150	The CSS Security Service shall provide an API to save/retrieve the ACL database onto persistent store.	DCCI	A	TC024.004	Test

C-CSS-21160	The CSS Security service shall provide the following APIs to MSS security management applications to retrieve/modify the access control lists associated with the ECS resources. a._to identify the permissions available to a principal b._to identify all the ACL managers protecting an object c._to get the printable representation of the permissions d._to locate the server with the writable copy of the ACL e._to read an ACL f._to write an ACL g._to test if the calling principal has some permissions h._to test if another principal has some permissions.	DCCI	A	TC024.004	Test
C-CSS-21170	The CSS Security service shall provide an API to maintain the integrity of the data passing between processes by using checksums at the following three levels: a._connect level b._request level c._packet level	DCCI	A	TC024.002	Test
C-CSS-21180	The CSS Security service shall provide an API to encrypt and send the data passing between processes at the following three levels: a._connect level b._request level c._packet level	DCCI	A	TC024.002	Test
C-CSS-21190	The CSS Security service shall provide an API to receive and decrypt the data passing between processes at the following three levels: a._connect level b._request level c._packet level	DCCI	A	TC024.002	Test
C-CSS-21200	The CSS Security service shall support the Data Encryption Standard (DES) to encrypt and decrypt data.	DCCI	A	TC024.002	Test

C-CSS-21210	The CSS Security service shall provide the capability to log audit information into security logs whenever authentication and authorization services are used. The audit information will contain the following: a._Date and time of the event b._User name c._Type of event d._Success or failure of the event e._Origin of the request	DCCI	A	TC024.010	Demo
C-CSS-22000	The CSS Message service shall provide an API for senders to send messages to receivers asynchronously without waiting for the receivers to receive it.	DCCI	A	TC023.003	Demo
C-CSS-22010	The CSS Message service shall provide an API for senders to send messages to receivers in a deferred synchronously manner through an intermediary whereby they can contact the intermediary at a latter time to receive the result.	DCCI	A	TC023.003	Test
C-CSS-22040	The CSS Message Service shall provide an API for the sender to designate multiple receivers for asynchronous messages.	DCCI	A	TC023.003	Test
C-CSS-22050	The CSS Message Service shall support multiple message queues so different groups of processes can use different message queues.	DCCI	A	TC023.003	Test
C-CSS-22060	The CSS Message Service shall purge a message from the message queue after a user specified time irrespective of its delivery to the receivers.	DCCI	A	TC023.003	Demo
C-CSS-22070	The CSS Message Service shall store undeliverable messages and retrieve and transmit them later.	DCCI	A	TC023.003	Demo
C-CSS-22080	The CSS Message Service shall provide an API for the receiver to register interest in receiving messages from a certain sender.	DCCI	A	TC023.003	Demo

C-CSS-22090	The CSS Message Service shall provide the capability to locate and send (push model) the messages to receivers.	DCCI	A	TC023.003	Test
C-CSS-22100	The CSS Message Service shall provide a non blocking API for the receiver to contact the message queue and get (pull model) the message.	DCCI	A	TC023.003	Demo
C-CSS-22110	The CSS Message service shall support guaranteed delivery of the message to the receiver.	DCCI	A	TC023.003	Test
C-CSS-22120	The CSS Message service shall provide an API for the sender of the message to get the acknowledgment information the message service receives from the receivers.	DCCI	A	TC023.003	Demo
C-CSS-22130	The CSS Message service shall associate the receiver to a returned value and maintain that information locally until the sender requests that information.	DCCI	A	TC023.003	Test
C-CSS-22140	The CSS Message Service shall provide an API for the sender of the message to receive return information stored at the message queue.	DCCI	A	TC023.003	Demo
C-CSS-22150	The CSS Message Service shall defer sending a message to a receiver, if the receiver is not active, and should try sending the message periodically with a set interval of time until the receiver is active.	DCCI	A	TC023.003	Test
C-CSS-23010	The CSS Event Service shall provide asynchronous communication between objects	DCCI	A	TC022.002	Demo
C-CSS-23020	The CSS Event Service shall provide a push API that allows a supplier of events to initiate the transfer of the event data to consumers.	DCCI	A	TC022.002	Demo
C-CSS-23030	The CSS Event Service shall provide a pull API that allows a consumer of events to request the event data from a supplier	DCCI	A	TC022.002	Test

C-CSS-23040	The CSS Event Service shall provide an intervening object that allows multiple suppliers to communicate with multiple consumers in a decoupled fashion.	DCCI	A	TC022.002	Test
C-CSS-23050	The CSS Event Service shall provide an API that communicates push event data to the consumer from a supplier by invoking the operation and passing the event data as a parameter.	DCCI	A	TC022.002	Test
C-CSS-23060	The CSS Event Service shall provide an API that terminates the push event communication between supplier and consumer.	DCCI	A	TC022.002	Test
C-CSS-23070	The CSS Event Service shall provide an API that blocks until the pull event data is available or an exception is raised. It returns the event data to the pull consumer.	DCCI	A	TC022.002	Test
C-CSS-23080	The CSS Event Service shall provide an API that terminates the pull event communication between supplier and consumer.	DCCI	A	TC022.002	Test
C-CSS-23090	The CSS Event Service shall provide an API that connects a push supplier to the intermediary for the push consumers.	DCCI	A	TC022.002	Test
C-CSS-23100	The CSS Event Service shall provide an API that connects a pull consumer to the intermediary for the pull suppliers.	DCCI	A	TC022.002	Test
C-CSS-23110	The CSS Event Service shall provide an API that connects a pull supplier to the intermediary for the pull consumers.	DCCI	A	TC022.002	Test
C-CSS-23120	The CSS Event Service shall provide an API that connects a push consumer to the intermediary for the push suppliers.	DCCI	A	TC022.002	Test
C-CSS-23130	The CSS Event Service shall provide an API that returns a proxy that is then used to connect a push-style consumer.	DCCI	A	TC022.002	Test

C-CSS-23140	The CSS Event Service shall provide an API that returns a proxy that is then used to connect a pull-style consumer.	DCCI	A	TC022.002	Test
C-CSS-23150	The CSS Event Service shall provide an API that returns a proxy that is then used to connect a push-style supplier.	DCCI	A	TC022.002	Test
C-CSS-23160	The CSS Event Service shall provide an API that returns a proxy that is then used to connect a pull-style supplier.	DCCI	A	TC022.002	Test
C-CSS-24010	The CSS Lifecycle Service shall provide a generic instantiation capability that creates a new object for a client.	DCCI	A	TC022.002	Test
C-CSS-24020	The CSS Lifecycle Service shall provide an API that accepts state initialization information.	DCCI	A	TC022.002	Demo
C-CSS-24030	The CSS Lifecycle Service shall provide an API that accepts resource preference information.	DCCI	A	TC022.002	Test
C-CSS-24040	The CSS Lifecycle Service shall provide an API that returns an object invocation handle.	DCCI	A	TC022.002	Test
C-CSS-24050	The CSS Lifecycle Service shall ensure that a server is available to service a user request.	DCCI	A	TC022.002	Test
C-CSS-24060	The CSS Lifecycle Service shall act as an intermediary during the client server connection phase.	DCCI	A	TC022.002	Demo
C-CSS-25010	The CSS Time Service shall adjust the time kept by the operating system at every node.	DCCI	A	TC023.006	Test
C-CSS-25020	The CSS Time Service shall be used to obtain timestamps that are based on Coordinated Universal Time (UTC).	DCCI	A	TC023.006	Demo
C-CSS-25030	The CSS Time Service shall provide an API to retrieve timestamp information.	DCCI	A	BC023.006	Demo
C-CSS-25040	The CSS Time Service shall provide an API for converting between binary timestamps that use different time structures.	DCCI	A	BC023.006	Demo

C-CSS-25050	The CSS Time Service shall provide an API for converting between binary timestamps and ASCII representations.	DCCI	A	BC023.006	Demo
C-CSS-25060	The CSS Time Service shall provide an API for converting between UTC time and local time.	DCCI	A	BC023.006	Demo
C-CSS-25070	The CSS Time Service shall provide an API for manipulating binary timestamps.	DCCI	A	BC023.006	Demo
C-CSS-25080	The CSS Time Service shall provide an API for comparing two binary time values.	DCCI	A	BC023.006	Demo
C-CSS-25090	The CSS Time Service shall provide an API for calculating binary time values.	DCCI	A	BC023.006	Demo
C-CSS-25100	The CSS Time Service shall provide an API for obtaining time zone information.	DCCI	A	BC023.006	Demo
C-CSS-25110	The CSS Time Service shall utilize a UTC based time provider.	DCCI	A	TC023.006	Demo
C-CSS-26010	The CSS Thread Service shall allow the option that each invocation of a server operation to run as a distinct thread.	DCCI	A	TC022.002	Demo
C-CSS-26020	The CSS Thread Service shall protect against conflicts between different threads accessing the same data.	DCCI	A	TC022.002	Demo Test
C-CSS-26030	The CSS Thread Service shall take into account the possibility that other threads may change shared data at any point. Code that will function correctly when executed by multiple concurrent threads is called thread-safe.	DCCI	A	TC022.002	Demo Test
C-CSS-26040	The CSS Thread Service shall provide an API that synchronizes the access of shared data between concurrent threads.	DCCI	A	TC022.002	Test
C-CSS-26050	The CSS Thread Service shall provide a synchronizing object that is in one of two states: locked or unlocked.	DCCI	A	TC022.002	Test
C-CSS-26060	The CSS Thread Service shall provide an API that allows each thread to lock the synchronizing object before it accesses the shared data.	DCCI	A	TC022.002	Test

C-CSS-26070	The CSS Thread Service shall provide an API that allows each thread to unlock the synchronizing object when it is finished accessing that data.	DCCI	A	TC022.002	Test
C-CSS-26080	The CSS Thread Service shall if the synchronizing object is locked by another thread, block the thread requesting the lock.	DCCI	A	TC022.002	Test
C-CSS-60300	The CSS File Access Service shall provide transparent access to remote files.	DCCI	A	TC020.003	Test
C-CSS-60310	The CSS File Access Service shall support access control for the remote files.	DCCI	A	TC020.003	Demo
C-CSS-60320	The CSS File Access Service shall provide location independent naming for the remote files.	DCCI	A	TC020.003	Demo
C-CSS-60800	The CSS File Access Service shall provide an option for scheduling file transfers in batch mode.	DCCI	A	TC020.004	Demo
C-CSS-60810	The CSS File Access Service shall log results of the non-interactive operations to operator specified log files.	DCCI	A	TC020.004	Demo
C-CSS-60820	The CSS File Access Service shall provide an option to send alarms and generate events if a scheduled operation fails.	DCCI	A	TC020.004	Demo
C-CSS-60900	The CSS File Access Service shall provide an API which allows applications to transfer files.	DCCI	A	TC020.001	Test
C-CSS-60910	The CSS File Access Service shall allow for file type selection (ASCII or Binary).	DCCI	A	TC020.001	Test
C-CSS-60920	The CSS File Access Service shall accept authentication information for file transfers.	DCCI	A	TC020.001	Demo
C-CSS-61010	The CSS Electronic Mail Service shall interoperate and exchange messages with external mail systems based on SMTP and X.400 protocols.	DCCI	A	TC021.001	Demo

C-CSS-61020	The CSS Electronic Mail Service shall be capable of sending and receiving the Multi-purpose Internet Mail Extensions (MIME) messages.	DCCI	A	TC021.001	Demo
C-CSS-61030	The CSS Electronic Mail Service shall use the existing X.400 gateway available at GSFC to support X.400 operations.	DCCI	A	TC021.001	Demo
C-CSS-61040	The CSS Electronic Mail Service shall provide translation between SMTP and X.400 protocol.	DCCI	A	TC021.001	Test
C-CSS-61060	The CSS Electronic Mail Service shall be accessible in non-interactive mode via API.	DCCI	A	TC021.001	Demo
C-CSS-61430	The CSS Electronic Mail Service shall allow attaching either text or binary files to a message.	DCCI	A	TC021.002	Demo
C-CSS-61440	The CSS Electronic Mail Service shall allow discarding message(s) from the MAILBOX without saving.	DCCI	A	TC021.002	Demo
C-CSS-61450	The CSS Electronic Mail Service shall have the capability to forward a message.	DCCI	A	TC021.002	Demo
C-CSS-61460	The CSS Electronic Mail Service shall allow cut/copy/paste/delete/undo operations in the editor.	DCCI	A	TC021.002	Demo
C-CSS-61470	The CSS Electronic Mail Service shall provide navigation methods to go the next or previous message in the MAILBOX or selected folder.	DCCI	A	TC021.002	Demo
C-CSS-61490	The CSS Electronic Mail Service shall provide the capability to search for keywords in messages.	DCCI	A	TC021.002	Demo
C-CSS-61500	The CSS Electronic Mail Service shall provide the capability to search the MAILBOX or a folder for keywords in title text.	DCCI	A	TC021.002	Demo
C-CSS-61510	The CSS Electronic Mail Service shall provide the capability to search the MAILBOX or folders for a specific author.	DCCI	A	TC021.002	Demo

C-CSS-61800	The CSS Electronic Mail Service shall provide the capability to send an electronic mail message non interactively from an application.	DCCI	A	TC021.003	Demo
C-CSS-61810	The CSS Electronic Mail Service shall allow attaching multiple text or binary files to the mail message.	DCCI	A	TC021.003	Test
C-CSS-61820	The CSS Electronic Mail Service shall accept a file name as input for the message text.	DCCI	A	TC021.003	Demo
C-CSS-62050	The CSS Bulletin Board Service shall host the user registration service.	DCCI	A	TC030.002	Demo
C-CSS-62060	The CSS Bulletin Board Service shall provide the capability for copying files.	DCCI	A	TC021.005	Demo
C-CSS-62070	The CSS Bulletin Board Service shall support download of ECS toolkits.	DCCI	A	TC021.004	Demo
C-CSS-62080	The CSS Bulletin Board Service shall collect and maintain access history and statistical information for the service.	DCCI	A	TC021.005	Demo
C-CSS-62130	The CSS Bulletin Board Service shall provide a "What's new" feature which informs the user of the new information available on the bulletin boards.	DCCI	A	TC021	Demo
C-CSS-62320	The CSS Bulletin Board Service shall allow user to select a subscribed bulletin board for viewing summary of all messages in it.	DCCI	A	TC021.005	Demo
C-CSS-62330	The CSS Bulletin Board Service shall provide the capability to respond to a message by sending the response to the bulletin board and/or to the author of the message and/or any other operator specified destination.	DCCI	A	TC021.005	Demo
C-CSS-62390	The CSS Bulletin Board Service shall allow attaching ASCII or binary files to a message.	DCCI	A	TC021.006	Demo

C-CSS-62800	The CSS Bulletin Board Service shall interface for the applications to post a message to bulletin boards.	DCCI	A	TC021.005	Demo
C-CSS-62810	The CSS Bulletin Board Service shall allow attaching ASCII and binary files to a message.	DCCI	A	TC021.006	Test
C-CSS-62820	The CSS Bulletin Board Service shall allow a message to be posted to multiple bulletin boards.	DCCI	A	TC021.006	Demo
C-CSS-63000	The CSS Virtual Terminal shall provide a virtual device which hides the physical terminal characteristics and handling conventions from both the operator and the server host.	DCCI	A	TC018.001	Demo
C-CSS-63010	The CSS Virtual Terminal shall provide means to enhance characteristics of the basic virtual device by mutual agreement between the two communicating parties (option negotiations).	DCCI	A	TC018.001	Demo
C-CSS-63020	The CSS Virtual Terminal shall be based on industry standards and accepted protocols (telnet).	DCCI	A	TC018.001	Demo
C-CSS-63030	The CSS Virtual Terminal shall be capable of supporting octet.	DCCI	A	TC018.001	Inspec.tion
C-CSS-63040	The CSS Virtual Terminal shall provide guest access to non-registered users to log into the ECS guest server.	DCCI	A	TC018.002	Inspec.tion
C-HRD-11000	The Enterprise Monitoring Server shall be physically and functionally identical to the Enterprise Communications Server in supporting the CSMS requirements.		A	TC032.001	Demotion
C-HRD-11005	The Enterprise Monitoring Server shall share data with the Local System Management Server in supporting the CSMS requirements.		A	TC032.001	Inspection
C-HRD-11010	The Enterprise Monitoring Server shall preserve DAAC autonomy of operations.		A	TC032.001	Inspection

C-HRD-11015	The Enterprise Monitoring Server shall host the MSS software configuration items to create, with the Enterprise Communications Server and Management Workstations, an enterprise management and coordination center for the ECS.		A	TC032.001	Inspection
C-HRD-11100	The Enterprise Monitoring Server processor shall include a dedicated terminal to be used as a local systems operations console.		A	TC032.001	Inspection
C-HRD-11105	The Enterprise Monitoring Server processor shall be capable of expansion with additional quantities and types of peripherals.		A	TC032.001	Inspection
C-HRD-11110	The Enterprise Monitoring Server processor shall be upgradeable/replaceable within the same product family without major software modification or replacement of any peripheral or attached component.		A	TC032.001	Inspection
C-HRD-11115	The Enterprise Monitoring Server processor shall meet the following capacity and functional requirements: a._POSIX compliant IEEE 1003.1 operating system (UNIX). b._Support two dual-attached FDDI connections.		A	TC032.001	Inspection
C-HRD-11300	The Enterprise Monitoring Server short-term data storage shall be compatible with POSIX compliant operating systems from several vendors.		A	TC032.001	Inspection
C-HRD-11305	The Enterprise Monitoring Server intermediate-term data storage shall provide a minimum of 2.039 gigabytes and shall be upgradeable to 4.078 gigabytes.		A	TC032.001	Inspection
C-HRD-11310	The Enterprise Monitoring Server intermediate-term data storage shall be compatible with the Local System Management Server short-term data storage.		A	TC032.001	Inspection

C-HRD-11315	The Enterprise Monitoring Server intermediate-term data storage shall support RAID level-5: striping with interleaved parity.		A	TC032.001	Inspection
C-HRD-11320	The Enterprise Monitoring Server intermediate-term data storage shall have the following hot swappable components: a._Disks b._PowerSupplies c._Fans d. _Disk-array controllers		A	TC032.001	Inspection
C-HRD-11325	The Enterprise Monitoring Server intermediate-term storage shall be cross-strapped with the Enterprise Communications Server intermediate-term data storage in supporting the CSMS requirements.		A	TC032.001	Inspection
C-HRD-11330	The Enterprise Monitoring Server intermediate-term data storage shall sustain 120 disk access/sec per second or better (4K block sizes).		A	TC032.001	Inspection
C-HRD-11335	The Enterprise Monitoring Server intermediate-term data storage shall be capable of archiving data to the ECS data server archive for long-term storage.		A	TC032.001	Inspection
C-HRD-11340	The Enterprise Monitoring Server long-term data storage shall provide a minimum of 5.634 gigabytes and shall be upgradeable to 11.268 gigabytes.		A	TC032.001	Inspection
C-HRD-11345	The Enterprise Monitoring Server long-term data storage shall adhere to ECS data server archival requirements for data storage and retrieval.		A	TC032.001	Inspection
C-HRD-11500	The Enterprise Monitoring Server peripheral disk drives shall provide a minimum of .371 gigabytes and shall be upgradeable to .742 gigabyte.		A	TC032.001	Inspection

C-HRD-11505	The Enterprise Monitoring Server peripheral disk drives shall be capable of retrieving data stored from both the enterprise monitoring server short and long-term data storage.		A	TC032.001	Inspection
C-HRD-11530	The Enterprise Monitoring Server peripherals shall support one tape drive.		A	TC032.001	Inspection
C-HRD-11535	The Enterprise Monitoring Server peripheral tape drive shall have the following characteristics: a._4mm Digital Audio Tape format b._Accept industry standard magnetic 4mm DAT (i.e. DDS-90) c._Data transfer rate of 200KB/sec		A	TC032.001	Inspection
C-HRD-11540	The Enterprise Monitoring Server tape drives shall be upgradeable/replaceable within the same product family.		A	TC032.001	Inspection
C-HRD-11565	The Enterprise Monitoring Server peripherals shall support one CD-ROM drive.		A	TC032.001	Inspection
C-HRD-11570	The Enterprise Monitoring Server peripheral CD-ROM drive shall have the following characteristic: a._Accept 600MB Compact Disk		A	TC032.001	Inspection
C-HRD-11575	The Enterprise Monitoring Server peripheral CD-ROM drives shall be upgradeable/replaceable within the same product family.		A	TC032.001	Inspection
C-HRD-12000	The Local Management Server shall be physically and functionally identical to the Local Communications Server in supporting the CSMS requirements.		A	TC032.002	Inspection
C-HRD-12005	The Local Management Server shall share data with the Enterprise Monitoring Server in supporting the CSMS requirements.		A	TC032.002	Inspection
C-HRD-12010	The Local Management Server shall manage only the local DAAC and preserve other DAAC autonomy of operations.		A	TC032.002	Inspection

C-HRD-12015	The Local Management Server shall host the MSS software configuration items to create, with the Local Communications Server and Management Workstations, a local system management center for each ECS DAAC.		A	TC032.002	Inspection
C-HRD-12100	The Local Management Server processor shall include a dedicated terminal to be used as a local systems operations console.		A	TC032.002	Inspection
C-HRD-12105	The Local Management Server processor shall be capable of expansion with additional quantities and types of peripherals.		A	TC032.002	Inspection
C-HRD-12110	The Local Management Server processor shall be upgradeable/replaceable within the same product family without major software modification or replacement of any peripheral or attached component.		A	TC032.002	Inspection
C-HRD-12115	The Local Management Server processor shall meet the following capacity and functional requirements: a._POSIX compliant IEEE 1003.1 operating system (UNIX). b._Support two dual-attached FDDI connections.		A	TC032.002	Inspection
C-HRD-12300	The Local Management Server short-term data storage shall be compatible with POSIX compliant operating systems from several vendors.		A	TC032.002	Inspection

C-HRD-12305	The Local Management Server short-term data storage shall provide a minimum of storage capacity for each DAAC configuration: a. _GSFC LSM: .515 gigabytes, upgradeable to 1.030 gigabytes b. _GSFC EOC: .459 gigabytes, upgradeable to .918 gigabytes c. _EDC LSM: .515 gigabytes, upgradeable to 1.030 gigabytes d. _LaRC LSM: .505 gigabytes, upgradeable to 1.010 gigabytes e. _MSFC LSM: .472 gigabytes, upgradeable to .944 gigabytes		A	TC032.002	Inspection
C-HRD-12310	The Local Management Server short-term data storage shall be compatible with the Enterprise Monitoring Server intermediate-term data storage.		A	TC032.002	Inspection
C-HRD-12315	The Local Management Server short-term data storage shall support RAID level-5: striping with interleaved parity.		A	TC032.002	Inspection
C-HRD-12320	The Local Management Server short-term data storage shall have the following hot swappable components: a._Disks b._PowerSupplies c._Fans d. _Disk-array controllers		A	TC032.002	Inspection
C-HRD-12325	The Local Management Server short-term data storage shall be cross-strapped with the Local Communications Server short-term data storage in supporting the CSMS requirements.		A	TC032.002	Inspection

C-HRD-12330	The Local Management Server short-term data storage shall sustain a disk access rate (4K block sizes) for each DAAC configuration: a. _GSFC LSM: 48 access/sec or better b. _GSFC EOC: 48 access/sec or better c. _EDC LSM: 51 access/sec or better d. _LaRC LSM: 188 access/sec or better e. _MSFC LSM: 38 access/sec or better		A	TC032.002	inspection
C-HRD-12335	The Local Management Server short-term data storage shall be capable of archiving data to the Enterprise Monitoring Server intermediate-term data storage.		A	TC032.002	Inspection
C-HRD-12500	The Local Management Server peripheral disk drives shall provide a minimum of .371 gigabytes and shall be upgradeable to .742 gigabytes.		A	TC032.002	Inspection
C-HRD-12505	The Local Management Server peripheral disk drives shall be capable of retrieving data stored from both the Local Management server short-term data storage.		A	TC032.002	Inspection
C-HRD-12530	The Local Management Server peripherals shall support one tape drive.		A	TC032.002	Inspection
C-HRD-12535	The Local Management Server peripheral tape drive shall have the following characteristics: a._4mm Digital Audio Tape format b._Accept industry standard magnetic 4mm DAT (i.e. DDS-90) c._Data transfer rate of 200KB/sec		A	TC032.002	Inspection
C-HRD-12540	The Local Management Server tape drives shall be upgradeable/ replaceable within the same product family.		A	TC032.002	Inspection
C-HRD-12565	The Local Management Server peripherals shall support one CD-ROM drive.		A	TC032.002	Inspection

C-HRD-12570	The Local Management Server peripheral CD-ROM drive shall have the following characteristic: a._Accept 600MB Compact Disk		A	TC032.002	Inspection
C-HRD-12575	The Local Management Server peripheral CD-ROM drives shall be upgradeable/replaceable within the same product family.		A	TC032.002	Inspection
C-HRD-13000	All Management Workstations and processors shall be capable of operating simultaneously and independently of other workstations and management/communications servers.		A	TC032.003	Inspection
C-HRD-13100	At a minimum, each processor shall meet the following capacity and functional requirements: a._POSIX compliant IEEE 1003.1 operating system (UNIX) b._Support AUI 802.3 ethernet connection. c._Provide 46 Mbyte of internal RAM.		A	TC032.003	Inspection
C-HRD-13105	Each Management Workstation shall provide one QWERTY keyboard which shall: a._Be detachable and cabled for movement on a desk-top style workstation area b._Provide a minimum of 12 programmable function keys		A	TC032.003	Inspection

C-HRD-13110	Each Management Workstation shall provide one color text and graphics display device which shall: a._Display the complete ASCII character set b._Provide a minimum of 1024 pixel x 864 lines resolution display c._Display a minimum of 16 colors d._Display pages 24 lines by 80 characters wide e._Display a minimum of four screen display pages f._Display pages readable from any location along the width of the workstation and up to a distance of 6 feet from the screen g._Provide a minimum of 19 inches diagonal non-glare screen h._Provide RGB video output for hard copy i._Feature an integral swivel/tilt base j._Provide brightness, contrast and power controls within easy reach. k._Be physically relocatable within the operations center		A	TC032.003	Inspection
C-HRD-13115	The Management Workstation shall provide one cursor pointing device (mouse)		A	TC032.003	Inspection
C-HRD-13120	The Management Workstation shall be upgradeable/replaceable within the same product family.		A	TC032.003	Inspection
C-HRD-13300	The Management Workstation data storage shall be capable of retrieving data from the data storage function of both the Enterprise Monitoring Server and the Local Management Server.		A	TC032.003	Inspection
C-HRD-13500	Management Workstation disk drives shall provide a minimum of .296 gigabytes and shall be upgradeable to .591 gigabytes.		A	TC032.003	Inspection

C-HRD-13505	All Management Workstation disk drives serving a specific function (e.g. local management, enterprise monitoring) shall be identical and will have equal capacity.		A	TC032.003	Inspection
C-HRD-13900	Each Printer shall be physically and functionally identical in supporting the CSMS printing requirements.		A	TC032.003	Inspection
C-HRD-16000	The Enterprise Monitoring Server shall be capable of 100 percent growth in processing speed without modifications or upgrades to software.		A	TC032.003	Inspection
C-HRD-16005	The Enterprise Monitoring Server shall be capable of 100 percent growth in storage capacity without modifications or upgrades to software.		A	TC032.003	Inspection
C-HRD-16010	The Local Management Server shall be capable of 100 percent growth in processing speed without modifications or upgrades to software.		A	TC032.003	Inspection
C-HRD-16015	The Local Management Server shall be capable of 100 percent growth in storage capacity without modifications or upgrades to software.		A	TC032.003	Inspection
C-HRD-17000	The MSS-MHCI hardware selection criteria shall meet overall ECS security policies and system requirements.		A	TC032.003	Inspection
C-HRD-18000	The MSS-MHCI Enterprise Monitoring Server shall maintain one backup of all software and key data items in a separate physical location.		A	TC032.001	Inspection
C-HRD-18005	The MSS-MHCI Local Management Server shall maintain one backup of all software and key data items in a separate physical location.		A	TC032.002	Inspection

C-HRD-18010	The MSS-MHCI functional string between the Enterprise Monitoring Server and the Local Management Server shall provide a function Ao (operational availability) of 0.998 and an MDT of 20 minutes.		A	TC032.001	Inspection
C-HRD-18015	The MSS-MHCI functional string between the Local Management Server and ECS managed objects shall provide a function Ao of 0.998 and an MDT of 20 minutes.		A	TC032.002	Inspection
C-HRD-21000	The Enterprise Communications Server shall be physically and functionally identical to the Enterprise Monitoring Server in supporting the CSMS requirements.		A	TC033.001	Inspection
C-HRD-21005	The Enterprise Communications Server shall share data with the Local Communications Server in supporting the CSMS requirements.		A	TC033.001	Inspection
C-HRD-21010	The Enterprise Communications Server shall preserve DAAC autonomy of operations.		A	TC033.001	Inspection
C-HRD-21015	The Enterprise Communications Server shall host the CSS software configuration items to create, with the Enterprise Monitoring Server and Management Workstations, an enterprise management and coordination center for the ECS.		A	TC033.001	Inspection
C-HRD-21100	The Enterprise Communications Server processor shall include a dedicated terminal to be used as a local systems operations console.		A	TC033.001	Inspection
C-HRD-21105	The Enterprise Communications Server processor shall be capable of expansion with additional quantities and types of peripherals.		A	TC033.001	Inspection

C-HRD-21110	The Enterprise Communications Server processor shall be upgradeable/replaceable within the same product family without major software modification or replacement of any peripheral or attached component.		A	TC033.001	Inspection
C-HRD-21115	The Enterprise Communications Server processor shall meet the following capacity and functional requirements: a._POSIX compliant IEEE 1003.1 operating system (UNIX). b._Support two dual-attached FDDI connections.		A	TC033.001	Inspection
C-HRD-21300	The Enterprise Communications Server intermediate-term data storage shall be compatible with POSIX compliant operating systems from several vendors.		A	TC033.001	Inspection
C-HRD-21305	The Enterprise Communications Server intermediate-term data storage shall provide a minimum of 2.039 gigabytes and shall be upgradeable to 4.078 gigabytes.		A	TC033.001	Inspection
C-HRD-21310	The Enterprise Communications Server intermediate-term data storage shall be compatible with the Communications Server short-term data storage.		A	TC033.001	Inspection
C-HRD-21315	The Enterprise Communications Server intermediate-term data storage shall support RAID level-5: striping with interleaved parity.		A	TC033.001	Inspection
C-HRD-21320	The Enterprise Communications Server intermediate-term data storage shall have the following hot swappable components: a._Disks b._PowerSupplies c._Fans d. _Disk-array controllers		A	TC033.001	Inspection
C-HRD-21325	The Enterprise Communications Server intermediate-term data storage shall be cross-strapped with the Enterprise Monitoring Server intermediate-term data storage in supporting the CSMS requirements.		A	TC033.001	Inspection

C-HRD-21330	The Enterprise Communications Server intermediate-term data storage shall sustain 120 disk access/sec per second or better (4K block sizes).		A	TC033.001	Inspection
C-HRD-21335	The Enterprise Communications Server intermediate-term data storage shall be capable of archiving data to the ECS Data Server archive for long-term storage.		A	TC033.001	Inspection
C-HRD-21340	The Enterprise Communications Server long-term data storage shall provide a minimum of 5.634 gigabytes and shall be upgradeable to 11.268 gigabytes.		A	TC033.001	Inspection
C-HRD-21345	The Enterprise Communications Server long-term data storage shall adhere to ECS data server archival requirements for data storage and retrieval.		A	TC033.001	Inspection
C-HRD-21500	The Enterprise Communications Server peripheral disk drives shall provide a minimum of .371 gigabytes and shall be upgradeable to .742 gigabyte.		A	TC033.001	Inspection
C-HRD-21505	The Enterprise Communications Server peripheral disk drives shall be capable of retrieving data stored from both the Enterprise Communications server short and long-term data storage.		A	TC033.001	Inspection
C-HRD-21530	The Enterprise Communications Server peripherals shall support one tape drive.		A	TC033.001	Inspection
C-HRD-21535	The Enterprise Communications Server peripheral tape drive shall have the following characteristics: a._4mm Digital Audio Tape format b._Accept industry standard magnetic 4mm DAT (i.e. DDS-90) c._Data transfer rate of 200KB/sec		A	TC033.001	Inspection
C-HRD-21540	The Enterprise Communications Server tape drives shall be upgradeable/replaceable within the same product family.		A	TC033.001	Inspection

C-HRD-21565	The Enterprise Communications Server peripherals shall support one CD-ROM drive.		A	TC033.001	Inspection
C-HRD-21570	The Enterprise Communications Server peripheral CD-ROM drive shall have the following characteristic: a._Accept 600MB Compact Disk		A	TC033.001	Inspection
C-HRD-21575	The Enterprise Communications Server peripheral CD-ROM drives shall be upgradeable/replaceable within the same product family.		A	TC033.001	Inspection
C-HRD-21900	The Enterprise Communications Server time source shall be a GFE NASA-36 bit serial time code signal synchronized to GMT.		A	TC033.001	Inspection
C-HRD-21905	The Enterprise Communications Server time source (via FOS) shall provide the master source to software-based time services throughout the ECS.		A	TC033.001	Inspection
C-HRD-22000	The Local Communications Server shall be physically and functionally identical to the Local Management Server in supporting the CSMS requirements.		A	TC033.002	Inspection
C-HRD-22005	The Local Communications Server shall share data with the Enterprise Communications Server in supporting the CSMS requirements.		A	TC033.002	Inspection
C-HRD-22010	The Local Communications Server shall be configurable according to local DAAC user authentication/authorization policy and preserve other DAAC autonomy of operations.		A	TC033.002	Inspection
C-HRD-22015	The Local Communications Server shall host the CSS software configuration items to create, with the Local Management Server and Management Workstations, a local system management center for each ECS DAAC.		A	TC033.002	Inspection

C-HRD-22100	The Local Communications Server processor shall include a dedicated terminal to be used as a local systems operations console.		A	TC033.002	Inspection
C-HRD-22105	The Local Communications Server processor shall be capable of expansion with additional quantities and types of peripherals.		A	TC033.002	Inspection
C-HRD-22110	The Local Communications Server processor shall be upgradeable/replaceable within the same product family without major software modification or replacement of any peripheral or attached component.		A	TC033.002	Inspection
C-HRD-22115	The Local Communications Server processor shall meet the following capacity and functional requirements: a._POSIX compliant IEEE 1003.1 operating system (UNIX). b._Support two dual-attached FDDI connections.		A	TC033.002	Inspection
C-HRD-22300	The Local Communications Server short-term data storage shall be compatible with POSIX compliant operating systems from several vendors.		A	TC033.002	Inspection
C-HRD-22305	The Local Communications Server short-term data storage shall provide a minimum of storage capacity for each DAAC configuration: a. _GSFC LSM: .515 gigabytes, upgradeable to 1.030 gigabytes b. _GSFC EOC: .459 gigabytes, upgradeable to .918 gigabytes c. _EDC LSM: .515 gigabytes, upgradeable to 1.030 gigabytes d. _LaRC LSM: .505 gigabytes, upgradeable to 1.010 gigabytes e. _MSFC LSM: .472 gigabytes, upgradeable to .944 gigabytes		A	TC033.002	Inspection

C-HRD-22310	The Local Communications Server short-term data storage shall be compatible with the Enterprise Communications Server intermediate-term data storage.		A	TC033.002	Inspection
C-HRD-22315	The Local Communications Server short-term data storage shall support RAID level-5: striping with interleaved parity.		A	TC033.003	Inspection
C-HRD-22320	The Local Communications Server short-term data storage shall have the following hot swappable components: a. _Disks b. _Power Supplies c. _Fans d. _Disk-array controllers		A	TC033.002	Inspection
C-HRD-22325	The Local Communications Server short-term data storage shall be cross-strapped with the Local Management Server short-term data storage in supporting the CSMS requirements.		A	TC033.003	Inspection
C-HRD-22330	The Local Communications Server short-term data storage shall sustain a disk access rate (4K block sizes) for each DAAC configuration: a. _GSFC LSM: 48 access/sec or better b. _GSFC EOC: 48 access/sec or better c. _EDC LSM: 51 access/sec or better d. _LaRC LSM: 188 access/sec or better e. _MSFC LSM: 38 access/sec or better		A	TC033.002	Inspection
C-HRD-22335	The Local Communications Server short-term data storage shall be capable of archiving data to the Enterprise Communications Server intermediate-term data storage.		A	TC033.002	Inspection
C-HRD-22500	The Local Communications Server peripheral disk drives shall provide a minimum of .371 gigabytes and shall be upgradeable to .742 gigabytes.		A	TC033.002	Inspection

C-HRD-22505	The Local Communications Server peripheral disk drives shall be capable of retrieving data stored from both the Local Communications server short and long-term data storage.		A	TC033.002	Inspection
C-HRD-22530	The Local Communications Server peripherals shall support one tape drive.		A	TC033.002	Inspection
C-HRD-22535	The Local Communications Server peripheral tape drive shall have the following characteristics: a._4mm Digital Audio Tape format b._Accept industry standard magnetic 4mm DAT (i.e. DDS-90) c._Data transfer rate of 200KB/sec		A	TC033.002	Inspection
C-HRD-22540	The Local Communications Server tape drives shall be upgradeable/replaceable within the same product family.		A	TC033.002	Inspection
C-HRD-22565	The Local Communications Server peripherals shall support one CD-ROM drive.		A	TC033.002	Inspection
C-HRD-22570	The Local Communications Server peripheral CD-ROM drive shall have the following characteristic: a._Accept 600MB Compact Disk		A	TC033.002	Inspection
C-HRD-22575	The Local Communications Server peripheral CD-ROM drives shall be upgradeable/replaceable within the same product family.		A	TC033.002	Inspection
C-HRD-22905	The Local Communications Server time source shall be slaved to the Enterprise Communications Server time source for software-based time services throughout the ECS.		A	TC033.002	Inspection
C-HRD-23000	The Bulletin Board Server shall share data with the Enterprise Communications Server in supporting the CSMS requirements.		A	TC033.003	Inspection

C-HRD-23005	The Bulletin Board Server shall preserve DAAC autonomy of operations and aggregate all ECS DAAC authentication/authorization policies by user type and DAAC, to provide a integrated view of ECS for user registration, account administration, and authentication/authorization to ECS services.		A	TC033.003	Inspection
C-HRD-23010	The Bulletin Board Server shall host the CSS software configuration items to create a single, secure unified access to all ECS services.		A	TC033.003	Inspection
C-HRD-23015	The Bulletin Board Server shall host ECS client software and toolkits for ECS-external distribution.		A	TC033.003	Inspection
C-HRD-23100	The Bulletin Board Server processor shall include a dedicated terminal to be used as a local systems operations console.		A	TC033.003	Inspection
C-HRD-23105	The Bulletin Board Server processor shall be upgradeable/expandable with additional quantities and types of peripherals.		A	TC033.003	Inspection
C-HRD-23110	The Bulletin Board Server processor shall be upgradeable/replaceable within the same product family without the need for any perturbation of any software or replacement of any peripheral or attached component.		A	TC033.003	Inspection
C-HRD-23115	The Bulletin Board Server processor shall meet the following capacity and functional requirements: a._POSIX compliant IEEE 1003.1 operating system (UNIX). b._Support FDDI connection.		A	TC033.003	Inspection
C-HRD-23300	The Bulletin Board Server intermediate-term data storage shall be compatible with POSIX compliant operating systems from several vendors.		A	TC033.003	Inspection

C-HRD-23305	The Bulletin Board Server intermediate-term data storage shall provide a minimum of 1.189 gigabytes, upgradeable to 2.378 gigabytes of storage capacity.		A	TC033.003	Inspection
C-HRD-23310	The Bulletin Board Server intermediate-term data storage shall be capable of archiving data to the ECS data server archive for long-term storage and software/toolkit safestore.		A	TC033.003	Inspection
C-HRD-23315	The Bulletin Board Server long-term data storage shall provide a minimum of 3 gigabytes, upgradeable to 6 gigabytes of storage capacity.		A	TC033.003	Inspection
C-HRD-23320	The Bulletin Board Server long-term data storage shall adhere to ECS data server archival requirements for data storage and retrieval.		A	TC033.003	Inspection
C-HRD-23530	The Bulletin Board Server peripherals shall support one tape drive.		A	TC033.003	Inspection
C-HRD-23535	The Bulletin Board Server peripheral tape drive shall have the following characteristics: a._4mm Digital Audio Tape format b._Accept industry standard magnetic 4mm DAT (i.e. DDS-90) c._Data transfer rate of 200KB/sec		A	TC033.003	Inspection
C-HRD-23540	The Bulletin Board Server tape drives shall be upgradeable/replaceable within the same product family.		A	TC033.003	Inspection
C-HRD-23565	The Bulletin Board Server peripherals shall support one CD-ROM drive.		A	TC033.003	Inspection
C-HRD-23570	The Bulletin Board Server peripheral CD-ROM drive shall have the following characteristic: a._Accept 600MB Compact Disk		A	TC033.003	Inspection
C-HRD-23575	The Bulletin Board Server peripheral CD-ROM drives shall be upgradeable/replaceable within the same product family.		A	TC033.003	Inspection

C-HRD-23905	The Bulletin Board Server time source shall be slaved to the Enterprise Communications Server time source for software-based time services throughout the ECS.		A	TC033.003	Inspection
C-HRD-27000	The CSS-DCHCI hardware selection criteria shall meet overall ECS security policies and system requirements.		A	TC033.003	Inspection
C-HRD-27005	The CSS-DCHCI Bulletin Board Server shall provide a security perimeter for ECS		A	TC033.003	Inspection
C-HRD-27010	The CSS-DCHCI Enterprise and Local Communications Servers shall be configured to provide autonomous DAAC security perimeters, FOS isolation, and an ISO CELL ECS security perimeter.		A	TC033.001 TC033.002	Inspection
C-HRD-28000	The CSS-DCHCI Enterprise Communications Server shall maintain one backup of all software and key data items in a separate physical location.		A	TC033.001	Inspection
C-HRD-28005	The CSS-DCHCI Local Communications Server shall maintain one backup of all software and key data items in a separate physical location.		A	TC033.002	Inspection
C-HRD-28010	The CSS-DCHCI functional string between the Enterprise Communications Server and the Local Communications Server shall provide a function Ao of 0.96 (.998 design goal) and an MDT of four hours (1.5 hour design goal).		A	TC033.001 TC033.002	Inspection
C-HRD-28015	The CSS-DCHCI functional string between the Local Communications Server and ECS clients to the Server shall provide a function Ao of 0.96 (.998 design goal) and an MDT of four hours (1.5 hour design goal).		A	TC033.001 TC033.002	Inspection

C-HRD-28020	The CSS DCHCI Enterprise Communications Server shall provide a function Ao of .998 (.999998 design goal) and an MDT of 20 minutes (design goal of 5 minutes) for all functions integral to providing a backup to the Enterprise Monitoring Server.		A	TC033.001	Inspection
C-HRD-28025	The CSS-DCHCI Enterprise Communications Server functions not integral to providing backup functionality to the Enterprise Monitoring Server shall provide a function Ao of 0.96 (.998 design goal) and an MDT of four hours (1.5 hour design goal).		A	TC033.001	Inspection
C-HRD-28030	The CSS DCHCI Local Communications Server shall provide a function Ao of .998 (.999998 design goal) and an MDT of 20 minutes (design goal of 5 minutes) for all functions integral to providing a backup to the Local Management Server.		A	TC033.002	Inspection
C-HRD-28035	The CSS-DCHCI Local Communications Server functions not integral to providing backup functionality to the Local Management Server shall provide a function Ao of 0.96 (.998 design goal) and an MDT of four hours (1.5 hour design goal).		A	TC033.002	Inspection
C-HRD-28040	The CSS-DCHCI Bulletin Board Server functions shall provide a function Ao of 0.96 (.998 design goal) and an MDT of four hours (1.5 hour design goal).		A	TC033.003	Inspection
C-HRD-31000	The ISS shall provide LANs at the following Release A sites: a._GSFC DAAC LAN b._GSFC EOC LAN c._EDC DAAC LAN d._LaRC DAAC LAN e._MSFC DAAC LAN		A	TC034.001	Inspection

C-HRD-32000	The ISS shall use physical devices and Medium Access Control protocols compatible with the following standards: a._IEEE 802.2 (Logical Link Control) b._IEEE 802.3 (MAC for Ethernet) c._IEEE 802.6 (MAC for SMDS) d._ANSI X3T9.5 (MAC for FDDI).		A	TC034.001	Inspection
C-HRD-32010	The ISS physical components, and services shall have the capability to be monitored via SNMP agents.		A	TC034.001	Inspection
C-HRD-34000	The LAN Analysis Equipment shall provide protocol analysis through the transport layer for all ISS LAN protocols and interconnection protocols to MANs/WANs.		A	TC034.001	Inspection
C-HRD-34010	The LAN Analysis Equipment shall include: a._One communications line monitor to store and display up to 10,000 bytes of data sent and received over any of the communications lines at rates of 10MB/sec to 100MB/sec, and supporting the protocols used within and interconnecting ECS. b._One digital VOM/multimeter c._One Local Area Network analyzer		A	TC034.001	Inspection
C-HRD-36000	The EOC LAN loop delay contribution shall not exceed more than TBD-(goal 250 msec) seconds of the total ECS delay of 2.5 seconds for emergency real-time commands.		A	TC034.002	Inspection
C-HRD-36010	The EOC Operational LAN backbone shall be able to support a peak traffic rate of 24 Mbps to support AM-1 flows from the Ecom interface.		A	TC034.002	Inspection

C-HRD-36020	The ISS shall provide wide area bandwidth necessary to support data transfer in accordance with Release A requirements specified in "Communications Requirements for the ECS Project", 194-220-SE3-001.		A	TC034.002	Inspection
C-HRD-36030	The ISS shall provide sufficient [TBD] local area network bandwidth at the LaRC DAAC to support data transfer between and among physical nodes provided by SDPS, MSS and CSS for Release A.		A	TC034.002	Inspection
C-HRD-36040	The ISS shall provide sufficient [TBD] local area network bandwidth at the MSFC DAAC to support data transfer between and among physical nodes provided by SDPS, MSS and CSS for Release A.		A	TC034.002	Inspection
C-HRD-36050	The ISS shall provide sufficient [TBD] local area network bandwidth at the GSFC DAAC to support data transfer between and among physical nodes provided by SDPS, MSS and CSS for Release A.		A	TC034.002	Inspection
C-HRD-36060	The ISS shall provide sufficient [TBD] local area network bandwidth at the EDC DAAC to support data transfer between and among physical nodes provided by SDPS, MSS and CSS for Release A.		A	TC034.002	Inspection
C-HRD-36070	The ISS LANs at the GSFC, MSFC and LaRC DAAC sites shall be capable of supporting (TBD) network traffic load estimates without redesign through Release B.		A	TC034.002	Inspection
C-HRD-36080	The ISS LANs at the Release-A DAAC sites shall be designed in a manner that allows a._Nodes to be added to any given LAN segment. b._Additional LAN segments to be added to the LAN.		A	TC034.002	Inspection

C-HRD-36090	The EOC Operational LAN shall be able to support 230 network devices without redesign.		A	TC034.002	Inspection
C-HRD-36100	The EOC Operational LAN shall be able to support peak data rates of up to 48 Mbps without redesign.		A	TC034.002	Inspection
C-HRD-37000	The ISS networks shall support the use of network and transport layer filtering to control access from internal and external interfaces		A	TC034.003	Inspection
C-HRD-39000	The ISS-INHCI DAAC LANs shall provide transparent portability across heterogeneous site LAN architectures.		A	TC034.003	Inspection
C-HRD-39005	The ISS-INHCI DAAC LANs shall enable expansion to GByte networks including the ability to provide increased volume of data distribution and access.		A	TC034.003	Inspection
C-HRD-41000	The EDF in the IR-1 timeframe shall provide a Enterprise Monitoring Server configured with: a._Two Fixed Disks b._One Tape Drive c._One CD-ROM Drive d._Storage cross-strapped with Enterprise Communications Server		A	TC035.001	Inspection
C-HRD-41005	The EDF in the IR-1 timeframe shall provide a Enterprise Communications Server configured with: a._Two Fixed Disks b._One Tape Drive c._One CD-ROM Drive d._One slaved Time Source e._Storage cross-strapped with Enterprise Monitoring Server		A	TC035.001	Inspection
C-HRD-41010	The EDF in the IR-1 timeframe shall provide a Bulletin Board Server configured with: a._One Tape Drive b._One CD-ROM Drive c. _One Fixed Drive		A	TC035.001	Inspection

C-HRD-41015	The EDF in the IR-1 timeframe shall provide two (2) intermediate-term Data Storage Unit supporting RAID level 5, one for the shared Enterprise Monitoring/Enterprise Communications, and the other for the Bulletin Board Server.		A	TC035.001	Inspection
C-HRD-41020	The EDF in the IR-1 timeframe shall provide two (2) Management Workstations, which can perform any EMC function.		A	TC035.001	Inspection
C-HRD-41025	The EDF in the IR-1 timeframe shall provide 1 system printer.		A	TC035.001	Inspection
C-HRD-41500	The EDF in the IR-1 timeframe infrastructure shall provide one EDF LAN.		A	TC035.001	Inspection
C-HRD-42000	The GSFC LSM in the IR-1 timeframe shall provide a Local Management Server configured with: a._Two Fixed Disks b._One Tape Drive c._One CD-ROM Drive		A	TC035.002	Inspection
C-HRD-42005	The GSFC LSM in the R-A timeframe shall provide a Local Communications Server configured with: a._Two Fixed Disks b._One Tape Drive c._One CD-ROM Drive d._One slaved Time Source e._Storage cross-strapped with Local Management Server		A	TC035.002	Inspection
C-HRD-42010	The GSFC LSM in the R-A timeframe shall provide one short-term Data Storage Unit supporting RAID level 5 cross strapped between the local management and local communications servers.		A	TC035.002	Inspection
C-HRD-42015	The GSFC LSM in the R-A timeframe shall provide two (2) Management Workstations, which can perform any EOC LSM function.		A	TC035.002	Inspection
C-HRD-42020	The GSFC LSM in the R-A timeframe shall provide 1 system printer.		A	TC035.002	Inspection

C-HRD-42500	The GSFC infrastructure in the R-A timeframe shall provide one GSFC LAN.		A	TC035.002	Inspection
C-HRD-42700	The GSFC EMC in the R-A timeframe shall provide an enterprise monitoring server, enterprise communications server, and bulletin board server transferred from the IR-1 EDF.		A	TC035.002	Inspection
C-HRD-42705	The GSFC EMC in the R-A timeframe shall provide, via the ECS data server a Enterprise Monitoring Server long-term data storage capability.		A	TC035.002	Inspection
C-HRD-43000	The EOC LSM in the R-A timeframe shall provide a Local Management Server configured with: a._Two Fixed Disks b._One Tape Drive c._One CD-ROM Drive d._Storage cross-strapped with Local Communications Server		A	TC035.002	Inspection
C-HRD-43005	The EOC LSM in the R-A timeframe shall provide a Local Communications Server configured with: a._Two Fixed Disks b._One Tape Drive c._One CD-ROM Drive d._One slaved Time Source e._Storage cross-strapped with Local Management Server		A	TC035.002	Inspection
C-HRD-43010	The EOC LSM in the R-A timeframe shall provide one short-term Data Storage Unit supporting RAID level 5 cross strapped between the local management and local communications servers.		A	TC035.002	Inspection
C-HRD-43015	The EOC LSM in the R-A timeframe shall provide two (2) Management Workstations, which can perform any EOC LSM function.		A	TC035.002	Inspection
C-HRD-43020	The EOC LSM in the R-A timeframe shall provide 1 system printer.		A	TC035.002	Inspection

C-HRD-43500	The EOC infrastructure in the R-A timeframe shall provide one EOC LAN.		A	TC035.002	Inspection
C-HRD-44000	The MSFC LSM in the IR-1 timeframe shall provide a Local Management Server configured with: a._Two Fixed Disks b._One Tape Drive c._One CD-ROM Drive		A	TC035.003	Inspection
C-HRD-44005	The MSFC LSM in the R-A timeframe shall provide a Local Communications Server configured with: a._Two Fixed Disks b._One Tape Drive c._One CD-ROM Drive d._One slaved Time Source e._Storage cross-strapped with Local Management Server		A	TC035.003	Inspection
C-HRD-44010	The MSFC LSM in the R-A timeframe shall provide one short-term Data Storage Unit supporting RAID level 5 cross strapped between the local management and local communications servers.		A	TC035.002	Inspection
C-HRD-44015	The MSFC LSM in the R-A timeframe shall provide two (2) Management Workstations, which can perform any EOC LSM function.		A	TC035.002	Inspection
C-HRD-44020	The MSFC LSM in the R-A timeframe shall provide 1 system printer.		A	TC035.002	Inspection
C-HRD-44500	The MSFC infrastructure in the R-A timeframe shall provide one MSFC LAN.		A	TC035.002	Inspection
C-HRD-45000	The LaRC LSM in the IR-1 timeframe shall provide a Local Management Server configured with: a._Two Fixed Disks b._One Tape Drive c._One CD-ROM Drive		A	TC035.003	Inspection

C-HRD-45005	The LaRC LSM in the R-A timeframe shall provide a Local Communications Server configured with: a._Two Fixed Disks b._One Tape Drive c._One CD-ROM Drive d._One slaved Time Source e._Storage cross-strapped with Local Management Server		A	TC035.002	Inspection
C-HRD-45010	The LaRC LSM in the R-A timeframe shall provide one short-term Data Storage Unit supporting RAID level 5 cross strapped between the local management and local communications servers.		A	TC035.002	Inspection
C-HRD-45015	The LaRC LSM in the R-A timeframe shall provide two (2) Management Workstations, which can perform any EOC LSM function.		A	TC035.002	Inspection
C-HRD-45020	The LaRC LSM in the R-A timeframe shall provide 1 system printer.		A	TC035.002	Inspection
C-HRD-45500	The LaRC infrastructure in the R-A timeframe shall provide one LaRC LAN.		A	TC035.002	Inspection
C-HRD-46000	The EDC LSM in the IR-1 timeframe shall provide a Local Management Server configured with: a._Two Fixed Disks b._One Tape Drive c._One CD-ROM Drive		A	TC035.003	Inspection
C-HRD-46005	The EDC LSM in the R-A timeframe shall provide a Local Communications Server configured with: a._Two Fixed Disks b._One Tape Drive c._One CD-ROM Drive d._One slaved Time Source e._Storage cross-strapped with Local Management Server		A	TC035.002	Inspection

C-HRD-46010	The EDC LSM in the R-A timeframe shall provide one short-term Data Storage Unit supporting RAID level 5 cross strapped between the local management and local communications servers.		A	TC035.002	Inspection
C-HRD-46015	The EDC LSM in the R-A timeframe shall provide two (2) Management Workstations, which can perform any EOC LSM function.		A	TC035.002	Inspection
C-HRD-46020	The EDC LSM in the R-A timeframe shall provide 1 system printer.		A	TC035.002	Inspection
C-HRD-46500	The EDC infrastructure in the R-A timeframe shall provide one EDC LAN.		A	TC035.002	Inspection
C-ISS-01020	The ISS shall interface with NSI or an alternate Internet provider at GSFC, MSFC, LaRC and EDC to provide DAAC access to science users in accordance with the following documents: a._DID 220, "Communications Requirements for the ECS Project" 194-220-SE3-001 b._Interface Requirements Document between EOSDIS Core System (ECS) and the NASA Science Internet (NSI), 194-219-SE1-001	NWCI	A	TC017.003	Demo
C-ISS-01030	The ISS shall provide connectivity between the MSFC DAAC and NOLAN for the ingest of L0 LIS data.	NWCI	A	TC017.001	Inspection Demo
C-ISS-01040	The ISS shall provide connectivity between the LaRC DAAC and NOLAN for the ingest of L0 CERES data.	NWCI	A	TC017.001	Demo
C-ISS-01080	The ISS shall reuse the V0 WAN in order to provide connectivity between V0 network nodes and V1 network nodes and provide interoperability between the systems.	NWCI	A	TC017.003	Demo

C-ISS-01090	The ISS shall provide local or metro area connectivity between V0 network nodes and V1 network nodes at GSFC, LaRC and MSFC DAAC sites in order to provide interoperability between the systems.	NWCI	A	BC017.003	Demo Inspection
C-ISS-01100	The ISS shall connect with TSDIS or with an exchange LAN to which TSDIS is attached in order to transfer TRMM data to the GSFC DAAC.	NWCI	A	TC017.003	Demo
C-ISS-01110	The ISS shall connect with TSDIS or with an exchange LAN to which TSDIS is attached in order to transfer TRMM data to the MSFC DAAC via the ESN WAN.	NWCI	A	TC017.003	Demo
C-ISS-01120	The ISS shall connect to the MSFC campus network to enable transfer of data between SCF(s) located at MSFC and the MSFC DAAC.	NWCI	A	TC017.003	Demo
C-ISS-01130	The ISS shall connect to the MSFC campus network to enable transfer of data between SCF(s) located at LaRC and the LaRCDAAC.	NWCI	A	TC017.003	Demo
C-ISS-01140	The ISS shall connect to the GSFC campus network to enable transfer of data between SCF(s) located at GSFC and the GSFC DAAC.	NWCI	IR1,A	TC017.003	Demo
C-ISS-01150	The ISS shall provide connectivity between the Landsat system and the EDC DAAC to support the ingest of Landsat data.	NWCI	A	TC017.003	Demo
C-ISS-01160	The ISS shall provide connectivity to the COLOR system and the GSFC DAAC to support the ingest of COLOR data.	NWCI	A	TC017.003	Demo
C-ISS-01170	The ISS shall provide connectivity between the EOC and Ecom for AM-1 interface testing.	NWCI	A	TC017.003	Demo

C-ISS-01180	The ISS shall provide connectivity between the EOC and the ESN Wide Area Network for AM-1 interface testing of EOC/IST communications.	NWCI	A	TC017.003 TC017.004	Demo
C-ISS-01190	The ISS shall provide LAN connectivity and OSI Layer 1 through Layer 4 services between EOC components (in support of FOS interface testing at Release A).	NWCI	A	TC017.004	Demo
C-ISS-01200	The topology of the EOC LANs shall not inhibit the reconfiguration of FOS devices to support either operational or support functions.	NWCI	A	TC017.004	Demo
C-ISS-01210	The ISS shall provide a separate network to support functions that will not interfere with the EOC's operational LAN.	NWCI	A	TC017.004	Test
C-ISS-01215	The EOC's support LAN architecture shall be identical in function and performance to that of the operational network.	NWCI	A	TC017.004	Testc
C-ISS-01220	The ISS shall provide LAN connectivity and OSI Layer 1 through Layer 4 services between SDPS components at the GSFC DAAC.	NWCI	A	TC017.003 TC017.004	Inspec Demo
C-ISS-01230	The ISS shall provide LAN connectivity and OSI Layer 1 through Layer 4 services between SDPS components at the LaRC DAAC.	NWCI	A	TC017.003 TC017.004	Demo
C-ISS-01240	The ISS shall provide LAN connectivity and OSI Layer 1 through Layer 4 services between SDPS components at the EDC DAAC.	NWCI	A	TC017.003 TC017.004	Demo
C-ISS-01250	The ISS shall provide LAN connectivity and OSI Layer 1 through Layer 4 services between SDPS components at the MSFC DAAC.	NWCI	A	TC017.003 TC017.004	Demo
C-ISS-01255	The ISS shall provide LAN connectivity and OSI Layer 1 through 4 services between CSMS components at the GSFC DAAC.	NWCI	A	TC017.003 TC017.004	Demo

C-ISS-01260	The ISS shall provide LAN connectivity and OSI Layer 1 through 4 services between CSMS components at the SMC.	NWCI	A	TC017.003 TC017.004	Demo
C-ISS-01270	The ISS shall provide LAN connectivity and OSI Layer 1 through 4 services between the SMC and the GSFC DAAC.	NWCI	A	TC017.003 TC017.004	Demo

C-ISS-01280	The ISS shall provide LAN connectivity and OSI Layer 1 through 4 services between the SMC and the EOC.	NWCI	A	TC017.003 TC017.004	Demo
C-ISS-01290	The ISS shall provide LAN connectivity and OSI Layer 1 through 4 services between the FOS EOC components and the CSMS-provided LSM within the EOC.	NWCI	A	TC017.003 TC017.004	Demo
C-ISS-01300	The ISS shall provide LAN connectivity and OSI Layer 1 through 4 services between the CSMS and the SDPS components at the MSFC DAAC.	NWCI	A	TC017.003 TC017.004	Demo
C-ISS-01310	The ISS shall provide LAN connectivity and OSI Layer 1 through 4 services between CSMS components at the MSFC DAAC.	NWCI	A	TC017.003 TC017.004	Demo
C-ISS-01320	The ISS shall provide LAN connectivity and OSI Layer 1 through 4 services between CSMS and SDPS components at the MSFC DAAC.	NWCI	A	TC017.003 TC017.004	Demo
C-ISS-01330	The ISS shall provide LAN connectivity and OSI Layer 1 through 4 services between CSMS components at the LaRC DAAC.	NWCI	A	TC017.003 TC017.004	Demo
C-ISS-01340	The ISS shall provide LAN connectivity and OSI Layer 1 through 4 services between CSMS and SDPS components at the LaRC DAAC.	NWCI	A	TC017.003 TC017.004	Demo
C-ISS-02000	The ISS shall provide connection oriented transport services as specified by the TCP protocol referenced in RFC 793.	NWCI	A	BC017.001	Demo
C-ISS-02010	The ISS shall provide the capability to filter packets based on the port/socket of the transport layer protocol.	NWCI	A	BC017.001	Demo Inspection
C-ISS-02020	The ISS shall provide connectionless transport services as specified by the UDP protocol referenced in RFC 768.	NWCI	A	BC017.001	Demo Inspection

C-ISS-02030	The ISS shall provide network layer services as specified by the Internet Protocol (IP) suite referenced in RFC 791.	NWCI	A	BC017.001	Demo Inspection
C-ISS-02040	The ISS shall provide the capability to filter packets based upon network layer source and/or destination addresses.	NWCI	A	BC017.001	Demo Inspection
C-ISS-02050	The ISS shall provide ICMP network layer service as specified by RFC 792.	NWCI	A	TC017.004	Demo
C-ISS-02060	The ISS shall provide network layer services in compliance with one or more of the following protocols as appropriate to the type of the physical network supported. a._IP over Ethernet as specified in RFCs 894, 895, 826 (ARP), 903 (RARP) b._IP over FDDI as specified in RFC 1188, 1390 (ARP, RARP) c._IP over HiPPI as specified in RFC 1374 (includes ARP, RARP) d._IP over SMDS as specified in RFC 1209 (includes ARP, RARP)	NWCI	A	TC017.004	Demo Inspection
C-ISS-02500	Using transport and network layer packet filtering, the EOC LAN shall be able to control access from both external and internal interfaces.	NWCI	A	TC017.005	Inspection Demo
C-ISS-02510	The EOC LAN shall be capable of supporting multicasting.	NWCI	A	TC017.004	Demo
C-ISS-02520	The ISS shall provide services based on the Open Shortest Path First (OSPF) protocol referenced in RFC 1583 to route traffic between the source and destination nodes, maintain route databases, and exchange routing information between networks.	NWCI	A	TC017.004	Demo
C-ISS-02530	The ISS shall provide services based on the Routing Information Protocol (RIP) referenced in RFC 1058 to route network traffic between the source and destination nodes.	NWCI	A	TC017.004	Demo Inspection

C-ISS-04000	The ISS LANs and WANs shall have an operapional availability of 0.96 at a minimum and an MDT of four (4) hours or less (1.5 hour design goal) unless otherwise specified.	NWCI	A	TC017.003 TC017.004 TC017.005 TC028.010	Demo Inspection
C-ISS-04010	For each ISS LAN segment or subnet, the operational availability and mean down time shall be sufficient to maintain the specified operational availability of the ECS functions it supports.	NWCI	A	TC017.004	Test Analysis
C-ISS-04020	Backups of all router configuration files shall be maintained at the local DAAC and the Network Management Facility (NMF).	NWCI	A	TC028.10	Testt
C-ISS-04030	Each ESN WAN point of presence shall have a primary and backup router.	NWCI	A	TC017.004	Demo Inspection
C-ISS-04040	The EOC LAN shall have no single point of failure for critical real-time functions.	NWCI	A	TC017.004 TC028.010	Demo Inspection
C-ISS-04050	The EOC Operational LAN shall provide the following levels of availability and mean down time (MDT): _for critical real-time data, .99980 availability, MDT < 1 minute;_ _for non-critical real-time data, .99925, MDT < 5 minutes.	NWCI	A	TC017.003 TC017.004 TC017.005 TC028.010	Demo Inspection
C-ISS-04055	The EOC Support LAN shall have an operational availability of at least 0.96 and shall have an MDT of no greater than 4 hours.	NWCI	A	TC017.003 - TC017.005 TC028.010	Test
C-ISS-04060	The portion of the DAAC LAN supporting the SDPS function of receiving science data shall have an operational availability of 0.999 at a minimum and an MDT of two (2) hours or less.	NWCI	A	TC017.003 - TC017.005 TC028.010	Test
C-ISS-04070	The portion of the DAAC LAN supporting the SDPS function of archiving and distributing data shall have an operational availability of 0.98 at a minimum and an MDT of two (2) hours or less.	NWCI	A	TC017.003 - TC017.005 TC028.010	Test

C-ISS-04080	The portion of the DAAC LAN supporting user interfaces to SDPS Client subsystem services shall have an operational availability of 0.993 at a minimum and an MDT of two (2) hours or less.	NWCI	A	TC017.003 - TC017.005 TC028.010	Test
C-ISS-04090	The portion of the DAAC LAN supporting the SDPS function of information searches on the ECS Directory shall have an operational availability of 0.993 at a minimum and an MDT of two (2) hours or less.	NWCI	A	TC017.003 - TC017.005 TC028.010	Test
C-ISS-04100	The portion of the DAAC LAN supporting the SDPS function of Data Acquisition Request (DAR) Submittal including TOOs shall have an operational availability of 0.993 at a minimum and an MDT of two (2) hours or less.	NWCI	A	TC017.003 - TC017.005 TC028.010	Test
C-ISS-04110	The portion of the DAAC LAN supporting the SDPS function of metadata ingest and update shall have an operational availability of 0.96 at a minimum and an MDT of four (4) hours or less.	NWCI	A	TC017.003 - TC017.005 TC028.010	Test
C-ISS-04120	The portion of the DAAC LAN supporting the SDPS function of information searches on local holdings shall have an operational availability of 0.96 at a minimum and an MDT of four (4) hours or less.	NWCI	A	TC017.003 - TC017.005 TC028.010	Test
C-ISS-04130	The portion of the DAAC LAN supporting the SDPS function of local data order submission shall have an operational availability of 0.96 at a minimum and an MDT of four (4) hours or less.	NWCI	A	TC017.003 - TC017.005 TC028.010	Test
C-ISS-04140	The portion of the DAAC LAN supporting the SDPS function of local data order submission across DAACs shall have an operational availability of 0.96 at a minimum and an MDT of four (4) hours or less.	NWCI	A	TC017.003 - TC017.005 TC028.010	Test

C-ISS-04150	The portion of the DAAC LAN supporting the SDPS subsystems data base management and maintenance interface shall have an operational availability of 0.96 at a minimum and an MDT of four (4) hours or less.	NWCI	A	TC017.003 - TC017.005 TC028.010	Test
C-ISS-06000	The ISS network architecture shall enable expansion to GByte networks including the ability to provide increased volume of data distribution/access.	NWCI	A	TC017.003 - TC017.005 TC028.010	Test
C-MSS-00010	The MSS services shall have an operational availability of .998 and an MDT of 20 minutes or less for critical services.	MCI	A	TC036.001	Demo
C-MSS-00020	The MSS services shall have no single point of failure for functions associated with network databases and configuration data.	MCI	A	TC036.001	Test
C-MSS-00030	The MSS services shall be extensible in its design to provide capability for growth and enhancement.	MCI	A	TC036.001	Test
C-MSS-00200	The MSS services shall allocate 10% of development resources for IV&V activity.	MCI	A	TC036.001	Test
C-MSS-10010	The MSS shall interface with the Ecom systems to exchange data identified in Table 5.1-1 as specified in the ECS/Ecom ICD.	MCI	A	BC031.012	Inspection
C-MSS-10020	The MSS shall interface with the Version 0 system to exchange data identified in Table 5.1-1 as specified in the ECS/V0 ICD 209-CD-011.	MCI	A	BC031.012	Test
C-MSS-10030	The MSS shall interface with the Science Computing Facility (SCF) to exchange data identified in Table 5.1-1 as specified in ECS/SCF ICD.	MCI	A	BC031.012	Test
C-MSS-10040	The MSS shall interface with the NASA Institutional Support System (NISS) to exchange data identified in Table 5.1-1 as specified in ECS/NISS ICD.	MCI	A	BC031.012	Test

C-MSS-10050	The MSS shall interface with the Affiliated Data Centers (ADC) to exchange data identified in Table 5.1-1 as specified in ECS/ADC ICD.	MCI	A	BC031.012	Test
C-MSS-10060	The MSS shall interface with the Tropical Rainfall Measuring Mission (TRMM) to exchange data identified in Table 5.1-1 as specified in ECS/TRMM ICD.	MCI	A	BC031.012	Test
C-MSS-10070	The MSS shall interface with the Landsat 7 System to exchange data identified in Table 5.1-1 as specified in ECS/Landsat 7 ICD.	MCI	A	BC031.012	Test
C-MSS-10080	The MSS shall interface with the NASA Science Internet (NSI) to exchange data identified in Table 5.1-1 as specified in ECS/NSI ICD.	MCI	A	BC031.012	Test
C-MSS-10090	The MSS shall interface with the Program Support Communications Network (PSCN) to exchange data identified in Table 5.1-1 as specified in ECS/PSCN ICD.	MCI	A	BC031.012	Test
C-MSS-10100	The MSS shall interface with the EDOS to exchange data identified in Table 5.1-1 as specified in ECS/EDOS ICD.	MCI	A	BC031.012	Test
C-MSS-10110	The MSS shall interface with the International Partners for Data Interoperability (IP) to exchange data identified in Table 5.1-1 as specified in ECS/IP ICD.	MCI	A	BC031.012	Test
C-MSS-10200	The MSS shall interface with the SDPS subsystems to exchange the data items in Table 5.1-2 as specified in the ECS internal ICDs, 313-DV3-003.	MCI	A	BC031.013	Test
C-MSS-10300	The MSS shall interface with the FOS subsystems to exchange the data items in Table 5.1-3 as specified in the ECS internal ICDs, 313-DV3-003.	MCI	A	BC031.013	Test
C-MSS-10400	The MSS at a site shall interface with the MSS subsystems at the SMC and other sites to exchange management data items in Table 5.1-4.	MCI	A	BC031.013	Test

C-MSS-10410	The MSS shall interface with the CSS subsystems to exchange the data items in Table 5.1-5 as specified in the ECS internal ICDs, 313-DV3-003.	MCI	A	BC031.013	Test
C-MSS-10420	The MSS shall interface with the ISS subsystems to exchange the data items in Table 5.1-6 as specified in the ECS internal ICDs, 313-DV3-003.	MCI	A	BC031.013	Test
C-MSS-12005	The MSS Management User Interface (MUI) Service shall be compatible with the ECS management framework.	MCI	A	TC028.009	Demo
C-MSS-12010	The MSS Management User Interface (MUI) Service shall provide a graphical user interface that is OSF/MOTIF compliant	MCI	A	TC028.009	Demo
C-MSS-12020	The MSS MUI Service shall have the capability to respond to keyboard and mouse input devices	MCI	A	TC028.009	Demo
C-MSS-12030	The MSS MUI Service shall provide a capability for the M&O Staff to add/delete a symbol and to modify a symbol's shape, color and position	MCI	A	TC028.009	Demo
C-MSS-12040	The MSS MUI Service shall provide a capability for an application to add/delete a symbol and to modify a symbol's shape, color and position	MCI	A	TC028.009	Demo
C-MSS-12050	The MSS MUI Service shall provide a capability for the M&O Staff to add, delete, and modify text strings	MCI	A	TC028.009	Demo
C-MSS-12060	The MSS MUI Service shall provide a capability for an application to add, delete, and modify text strings	MCI	A	TC028.009	Demo
C-MSS-12070	The MSS MUI Service shall have the capability to provide options and methods to the M&O Staff for screen configuration changes (color, symbol placement, etc) and for retaining the changes from session to session	MCI	A	TC028.009	Demo

C-MSS-12080	The MSS MUI Service shall provide a capability for an applications to alert the M&O Staff	MCI	A	TC028.009	Demo
C-MSS-12090	The MSS MUI Service shall provide a capability for an applications to establish a dialog session with the M&O Staff	MCI	A	TC028.009	Demo
C-MSS-12100	The MSS MUI Service shall provide a capability for the M&O Staff to load and unload vendor MIB.	MCI	A	TC028.009	Demo
C-MSS-12110	The MSS MUI Service shall provide a capability for an applications to load and unload vendor MIB	MCI	A	TC028.009	Demo
C-MSS-12120	The MSS MUI Service shall provide a capability for the operator to browse MIB values.	MCI	A	TC028.009	Demo
C-MSS-12130	The MSS MUI Service shall provide the capability for the M&O Staff to register and unregister managed objects. Managed objects will include network devices and ECS host systems in IR-1	MCI	A	TC028.009	Demo
C-MSS-12140	The MSS MUI Service shall provide the capability to register and unregister managed objects.	MCI	A	TC028.009	Demo
C-MSS-12170	The MSS MUI Service shall provide the capability to register and unregister management applications.	MCI	A	TC028.009	Demo
C-MSS-12180	The MSS MUI Service shall provide the capability for an application to display on-line help windows	MCI	A	TC028.009	Demo
C-MSS-14010	The MSS Maps/Collection Service shall retain the status of managed objects and their relationship to symbols that comprise a graphical representation of the physical network topology.	MCI	A	TC028.009	Demo
C-MSS-14020	The MSS Map/Collection Service shall provide a capability to define maps and objects.	MCI	A	TC028.009	Demo

C-MSS-14030	The MSS Map/Collection Service shall provide a capability to define a hierarchical relationship between maps and sub-maps (i.e., a graphical hierarchical tree)	MCI	A	TC028.009	Demo
C-MSS-14040	The MSS Map/Collection Service shall propagate events associated with objects up the hierarchical tree	MCI	A	TC028.009	Demo
C-MSS-16005	The ECS management protocol shall be the SNMP standard as specified in RFC 1157.	MCI	A	TC028.009	Demo
C-MSS-16010	MSS Monitor/Control Service shall communicate via ECS management protocol with the Management Agent Service in test or operational mode.	MCI	A	TC028.009	Inspec.
C-MSS-16020	The MSS Monitor/Control Service shall communicate via ECS management protocol with the MSS Management Agent Service to request performance and fault data on a managed object.	MCI	A	TC028.009	Demo
C-MSS-16030	The MSS Monitor/Control Service shall be able to communicate via ECS management protocol with the MSS Management Agent Service to send ECS management set messages to configure and control the processing performed by the ECS management agent.	MCI	A	TC028.009	Demo
C-MSS-16040	The MSS Monitor/Control Service shall communicate via ECS management protocol with the MSS Management Agent Service to receive ECS management traps/events.	MCI	A	TC028.009	Demo
C-MSS-16050	The MSS Monitor/Control Service shall allow customized M&O staff-event notifications and automatic actions.	MCI	A	TC028.009	Test
C-MSS-16060	The MSS Monitor/Control Service shall allow the capability to set thresholds on managed resources that are monitored	MCI	A	TC028.009	Test

C-MSS-16070	The MSS Monitor/Control Service shall automatically report when a threshold has been exceeded by generating a ECS management event	MCI	A	TC028.009	Demo
C-MSS-16100	The MSS Monitor/Control Service shall perform the following protocol test on managed network nodes: a._IP test b._TCP test c._SNMP test	MCI	A	TC028.009	Demo
C-MSS-18040	The MSS Management Data Access Service shall maintain the integrity of the management database.	MCI	A	BC031.009	Demo
C-MSS-18050	The MSS Management Data Access Service shall utilize CSS Services to access/transfer management data	MCI	A	BC031.009	Analysis
C-MSS-18060	The Management Data Access Service shall provide the capability for applications access to management data.	MCI	A	BC031.009	Test
C-MSS-18070	The MSS Management Data Access Service shall provide the capability to selectively access management data	MCI	A	BC031.009	Test
C-MSS-18200	The MSS Management Data Access Service shall provide the capability for an application via APIs to update fields in the management database	MCI	A	BC031.009	Demo
C-MSS-18220	The MSS Management Data Access Service shall provide the capability for an application via APIs to alter tables and fields in the management database	MCI	A	BC031.009	Test
C-MSS-18260	The MSS Management Data Access Service shall have the capability to schedule the transfer and loading log files into the management database at the site.	MCI	A	BC031.009	Test
C-MSS-18270	The MSS Management Data Access Service shall have the capability to schedule the archiving of log files at the site.	MCI	A	BC031.009	Demo

C-MSS-18280	The MSS Management Data Access Service shall schedule the transfer of management data at the sites to the SMC.	MCI	A	BC031.009	Demo
C-MSS-18330	The MSS Management Data Access Service shall provide the capability for an applications to append records to a log file.	MCI	A	BC031.009	Demo
C-MSS-18340	The MSS Management Data Access Service shall provide the capability for an application to selectively read a record from a log file	MCI	A	BC031.009	Test
C-MSS-18350	The MSS Management Data Access Service shall provide the capability for an application to load log files into the management database at the site	MCI	A	BC031.009	Test
C-MSS-20010	The MSS Discovery Service shall discover (via network protocol) new instances of managed objects.	MCI	A	TC028.009	Demo
C-MSS-20020	The MSS Discovery Service shall detect missing occurrences of managed objects	EMCI	A	TC028.009	Demo
C-MSS-20030	The MSS Discovery Service shall report missing occurrences of managed objects.	MCI	A	TC028.009	Demo
C-MSS-20040	The MSS Discovery Service shall update the object database after the Discovery Service receives a request to register/unregister a managed object.	MCI	A	TC028.009	Demo
C-MSS-36010	The MSS Management Agent Service shall retrieve data from ECS managed objects in test or operational mode.	MACI	A	TC029.007	Demo
C-MSS-36020	The MSS Management Agent Service shall communicate via ECS management protocol with the MSS Monitor/Control Service to respond to requests for managed object MIB attributes	MACI	A	TC029.007	Demo

C-MSS-36040	The MSS Management Agent Service shall communicate via ECS management protocol with the MSS Monitor/Control Service to send ECS management traps/events to the Monitor/Control Service.	MACI	A	TC029.007	Demo
C-MSS-36050	The MSS Management Agent Service shall communicate via ECS management protocol with the MSS Monitor/Control Service to receive ECS management set message from the Monitor/Control Service.	MACI	A	TC029.007	Test
C-MSS-36060	The MSS Management Agent Service shall provide an ECS management agent that is configurable to include: a._Community to respond to and set attributes b._Agent location & contact person c._Traps to send d._Events to log & log file name	MACI	A	TC029.007	Demo
C-MSS-36070	The MSS Management Agent Service shall provide an ECS management agent for network devices	MACI	A	TC029.007	Demo
C-MSS-36080	The MSS Management Agent Service shall provide an extensible ECS management agent for ECS Host systems	MACI	A	TC029.007	Test
C-MSS-36090	The MSS Management Agent Service shall provide an extensible ECS management agent for ECS applications	MACI	A	TC029.007	Test
C-MSS-36100	The MSS Management Agent Service shall provide proxy agents for ECS network devices and applications that cannot be managed via SNMP	MACI	A	TC029.007	Test
C-MSS-36110	The MSS Management Agent Service shall provide an ECS domain manager agent to coordinate and communicate with multiple ECS management agents	MACI	A	TC029.007	Test

C-MSS-40000	The MSS configuration management application service at each site shall maintain a name and unique identifier for the following ECS controlled items at the site: a._the ECS and each of its subsystems, networks, workstations, servers, and services; b._each ECS release, baseline, and operating environment deployed to the site from the EMC; c._specifications; d._each ECS custom computer software configuration item and its components; (IR-1) e._each ECS COTS computer software configuration item and its components; f._each ECS hardware configuration item and its components; g._technical documentation and test materials; (IR-1) h._each of the site's baselines and operating environments; i._scientific algorithm software; (IR-1, DAACs only) j._algorithm processing logic control and calibration coefficients data; (IR-1, DAACs only) k._algorithm test documentation, including specifications, data files, and scripts; (IR-1, DAACs only) l._facility layout drawings and documents; m._configured system and network devices.	MLCI	A	TC027	Test

C-MSS-40010	The MSS configuration management application service at each site shall specify the baseline, release, and operating environment associations among: a._ECS software, specifications, and documentation; b._scientific algorithm software (IR1, DAACs only); c._algorithm processing logic control and calibration coefficients data (IR1, DAACs only); d._ECS operational (system and site) releases, baselines, and operating environments; e._algorithm test documentation, including specifications, data files, and script. (IR1, DAACs only)	MLCI	A	TC0027	Inspection
C-MSS-40030	The MSS configuration management application service at each site shall identify, and report to the EMC, operational baselines at the site.	MLCI	A	TC027.005	Demo
C-MSS-40040	The MSS configuration management application service at each site shall maintain, and make available to the EMC, "level of assembly" descriptions of operational baselines at the site.	MLCI	A	TC027.005	Demo
C-MSS-40050	The MSS configuration management application service at each site shall maintain, and make available to the EMC, information identifying the versions and implementation status of configuration-controlled items at the site.	MLCI	A	TC027.005	Inspection

C-MSS-40060	The MSS configuration management application service at each site shall maintain historical status records for ECS and algorithm software at the site, including the software's: a._current version; b._current version's specifications and technical, operations, and maintenance documentation; c._documentation history; d._"level of assembly" description of the components that comprise it e._history of changes, including changes to subordinate units/components;	MLCI	A	TC027.005	Demo
C-MSS-40070	The MSS configuration management application service at the EMC and the sites shall maintain records that establish traceability among operational baselines and releases.	MLCI	A	TC027.005	Demo
C-MSS-40080	The MSS configuration management application service at the EMC and the sites shall maintain "level of assembly" descriptions of controlled item components.	MLCI	A	TC027.005	Demo
C-MSS-40100	The MSS configuration management application service at the SMC and the DAACs shall maintain SCF-provided configuration data for individual algorithms, including: a._algorithm development version numbers, identification codes, and reference numbers; b._SCF point of contact's name and organization; c._associated files' names, formats, sizes, and descriptions; d._number of files by category and type. (IR-1)	MLCI	A	TC027.004	Demo Inspection
C-MSS-40110	The MSS configuration management application service shall display and report indentured, "level of assembly" lists that describe the component structure of controlled items.	MLCI	A	TC027.005	Demo

C-MSS-40120	The MSS configuration management application service at the SMC shall maintain, and make available system-wide, a name and unique identifier for ECS configuration-controlled items, including: a._the ECS and each of its subsystems; b._ECS system-wide releases, baselines, and operating environments; c._ specifications; d._ECS computer software configuration items and their components, both custom and COTS; d._ECS hardware configuration items and their components; e._technical documentation and test materials; f._ECS operational (system and site) releases, site baselines, and operating environments; g._scientific algorithm software; h._algorithm processing logic control and calibration coefficients data; i._algorithm test documentation, including specifications, data files, and scripts.	MLCI	A	TC027.007	Demo
C-MSS-40140	The MSS configuration management application service at the SMC shall maintain, and make available system-wide, information identifying the sites where individual versions of controlled items are located and the operational status of that version at the site.	MLCI	A	TC027.007	Demo
C-MSS-40150	The MSS configuration management application service at the SMC shall maintain, and make available system-wide, records that identify the current and previous versions of ECS hardware and software resources deployed to the sites.	MLCI	A	TC027.007	Demo

C-MSS-40160	The MSS configuration management application service at the SMC shall maintain records that identify the current and previous versions of ECS documents deployed to the sites.	MLCI	A	TC027.007	Demo
C-MSS-40170	The MSS configuration management application service at the SMC shall maintain, and distribute to each site, records that identify the baseline changes included in each release of hardware and software deployed to the site.	MLCI	A	TC027.007	Demo
C-MSS-40180	The MSS configuration management application service at the SMC shall maintain, and distribute to each site, records that identify specifications and technical, operations, and maintenance documentation for each version of ECS hardware and software resources deployed to the site.	MLCI	A	TC027.007	Demo
C-MSS-40190	MSS configuration management application service at the SMC shall maintain, and distribute to each site, records that describe the change requests (enhancements and corrections) satisfied by new versions of ECS hardware, software, and documentation deployed to the sites.	MLCI	A	TC027.007	Demo

C-MSS-40200	The MSS configuration management application service at the SMC shall maintain historical status accounting records for each ECS-developed resource, to include: a._current version; b._current version's specifications and technical, operations, and maintenance documentation; c._documentation history; d._"level of assembly" description of the components that comprise it; e._history of changes, including changes to subordinate units/components; f._release configuration, including the configuration of its subordinate units/components.	MLCI	A	TC027.007	Demo
C-MSS-40210	The MSS configuration management application service at the SMC shall maintain historical status records for ECS releases, to include each release's: a._latest baseline plus approved changes. b._baseline history. c._latest release documentation. d._"level of assembly" description of the components that comprise it. e._history of changes, including changes to subordinate units/components. f._effectivity and installation status at operational sites. g._release configuration, including the configuration of its subordinate units/components.	MLCI	A	TC027.007	Demo Test
C-MSS-40220	The MSS configuration management application service at the SMC shall maintain historical status records of ECS baseline changes to include: a._sites affected; b._installation schedule; c._installation status.	MLCI	A	TC027.007	Test Demo Analysis

C-MSS-40240	The MSS configuration management application service at the SMC shall maintain software-critical and security-sensitive items lists.	MLCI	A	TC027.007	Test Demo
C-MSS-40250	The MSS configuration management application service at the SMC shall report, and make available system-wide, the identity and change status of documents associated with deployed ECS resources.	MLCI	A	TC027.007	Demo Inspection
C-MSS-40260	The MSS configuration management application service at the SMC shall report, and make available system-wide, the identity and change status of individual ECS resources deployed to the sites.	MLCI	A	TC027.007	Demo
C-MSS-40270	The MSS configuration management application service at the SMC shall report, and make available system-wide, the identity of resources comprising ECS baselines and releases.	MLCI	A	TC027.007	Demo
C-MSS-40280	The MSS configuration management application service shall characterize ECS-controlled resources as system-wide or site specific	MLCI	A	TC027.006	Demo
C-MSS-40290	The MSS configuration management application service shall accept and store baseline management data records provided via interactive user interface adn formatted data files	MLCI	A	TC027.006	Demo
C-MSS-40300	The MSS configuration management application service shall produce formatted data files containing baseline management data records	MLCI	A	TC027.006	Demo

C-MSS-40400	The MSS configuration management application service at the DAACs shall store scientific algorithm and ECS files that contain: a._source code; b._patches; c._control data, including coefficients and calibration data; d._scripts; e._designs and design specifications; f._databases; g._binaries and executables; h._technical documentation (both text and graphics); i._test data; j._test reports; k._interface specifications; l._configuration data. (IR-1)	MLCI	A	TC027.001	Demo
C-MSS-40410	The MSS configuration management application service at each DAAC shall maintain user-definable software configuration status information for each algorithm. (IR-1)	MLCI	A	TC027.001	Inspection
C-MSS-40420	The MSS configuration management application service at each site shall maintain M&O staff-definable software configuration status information for each version of every controlled file.	MLCI	A	TC027.001	Demo
C-MSS-40440	The MSS configuration management application service at the DAACs shall provide access to the SDPS process integration and test service for checkout and checkin of algorithms and associated data files and for construction of builds.	MLCI	A	TC027.006	Test

C-MSS-40460	The MSS configuration management application service at the SMC shall assemble unlicensed toolkit software files for posting to the ECS bulletin board. Files consist of: a._source code; b._linkable object code for selected workstation configurations; c._makefiles that automate installation; d._installation instructions.	MLCI	A	TC027.001	Demo
C-MSS-40470	The MSS configuration management application service shall regulate operations on library files through use of individual and group permissions.	MLCI	A	TC027.001	Demo
C-MSS-40480	The MSS configuration management application service shall use a checkout/edit/checkin paradigm to govern changing of controlled files.	MLCI	A	TC027.001	Demo
C-MSS-40490	The MSS configuration management application service shall track each controlled file that has been changed as a new version of the original file.	MLCI	A	TC027.001	Demo
C-MSS-40500	The MSS configuration management application service shall merge versions of controlled files.	MLCI	A	TC027.001	Demo
C-MSS-40510	The MSS configuration management application service shall maintain records of actual changes made to ECS resources in implementing system enhancement requests.	MLCI	A	TC027.001	Demo
C-MSS-40520	The MSS configuration management application service shall verify that changes to controlled resources are supported by valid, approved change requests.	MLCI	A	TC027.001	Demo

C-MSS-40530	The MSS configuration management application service shall identify implementation status for each version of every site-controlled item, reflecting the lifecycle stage to which it has been promoted.	MLCI	A	TC027.006	Demo
C-MSS-40540	The MSS configuration management application service shall automate build processes such that builds of baseline systems can be repeated and be used across a variety of platforms.	MLCI	A	TC027.001	Demo
C-MSS-40550	The MSS configuration management application service shall reconstruct previous versions of controlled files.	MLCI	A	TC027.001	Demo
C-MSS-40560	The MSS configuration management application service shall allow concurrent user access to controlled files.	MLCI	A	TC027.001	Demo
C-MSS-40570	The MSS configuration management application service shall maintain an audit trail of all changes made to controlled files.	MLCI	A	TC027.001	Demo
C-MSS-40600	The MSS configuration management application service shall provide a capability with which to compose ECS requests for system changes.	MLCI	A	TC027.003	Demo
C-MSS-40610	The MSS configuration management application service shall store copies of that site's proposed and approved requests to enhance or otherwise modify ECS components and configurations.	MLCI	A	TC027.003	Demo
C-MSS-40620	The MSS configuration management application service at the sites shall provide a capability with which to forward requests for ECS system changes to the EMC.	MLCI	A	TC027.003	Demo
C-MSS-40650	The MSS configuration management application service at the SMC shall receive change requests in electronic form from the sites.	MLCI	A	TC027.003	Demo

C-MSS-40660	The MSS configuration management application service at the SMC shall distribute change evaluation requests to designated organizations system-wide.	MLCI	A	TC027.003	Demo
C-MSS-40670	The MSS configuration management application service at the SMC shall receive and store impact assessments in response to change evaluation requests.	MLCI	A	TC027.003	Demo
C-MSS-40680	The MSS configuration management service at the SMC shall electronically link impact assessments to their associated change requests.	MLCI	A	TC027.003	Demo
C-MSS-40690	The MSS configuration management application service at the SMC shall maintain the status of responses to change evaluation requests.	MLCI	A	TC027.003	Demo
C-MSS-40700	The MSS configuration management application service at the SMC shall record summaries of impact assessments received.	MLCI	A	TC027.003	Demo
C-MSS-40720	The MSS configuration management application service at the SMC shall make change requests, assessments, and status available for system-wide viewing.	MLCI	A	TC027.003	Demo
C-MSS-40730	The MSS configuration management application service at the SMC shall maintain a historical record of ECS system impact assessments.	MLCI	A	TC027.003	Demo
C-MSS-40750	The MSS configuration management application service at the SMC shall track the approval status of each proposed change.	MLCI	A	TC027.003	Demo
C-MSS-40760	The MSS configuration management application service at the SMC shall report, and make available system-wide lists of the identity and disposition of changes proposed to the ECS.	MLCI	A	TC027.003	Demo

C-MSS-40770	The MSS configuration management application service at the SMC shall collect, and make available system-wide, the allocations, schedules and status of tasks for implementing CCB-approved changes to ECS hardware and software and for correcting non-conformance with system requirements	MLCI	A	TC027.004	Demo
C-MSS-40990	The MSS configuration management application service shall log the following information for configuration management events: a._operation type. b._userid of initiator. c._date-time stamp. d._host name. (IR-1, at the sites only)	MLCI	A	TC027.006	Demo
C-MSS-40995	The MSS configuration management application service shall generate chronological reports of logged CM events associated with M&O staff-selectable: a._time frames. b._operation types. c._userids. d._hosts (IR-1, at the sites only)	MLCI	A	TC027.006	Demo
C-MSS-60010	The MSS Fault Management Application Service shall provide the capability to create and display graphical representations of a given network topology consisting of the following: _a._routers _b._communication lines _c._hosts _d._peripherals _e._applications	MCI	A	TC029.001	Demo
C-MSS-60020	The MSS Fault Management Application Service shall provide the capability to define categories of faults.	MCI	A	TC029.001	Demo
C-MSS-60030	The MSS Fault Management Application Service shall provide the capability to assign faults to categories._	MCI	A	TC029.001	Demo

C-MSS-60040	The MSS Fault Management Application Service shall provide the capability to assign severity levels to faults._	MCI	A	TC029.001	Demo
C-MSS-60050	The MSS Fault Management Application Service shall be capable of providing the Management Data Access Service with a configurable list of fault categories that specify whether to enable or disable the logging of fault notifications for that fault category._	MCI	A	TC029.001	Demo
C-MSS-60060	The MSS Fault Management Application Service shall provide the capability to enable or disable the display of fault notifications received from a specific managed object based on fault category assigned to that fault._	MCI	A	TC029.001	Demo
C-MSS-60070	The MSS Fault Management Application Service shall provide the capability to specify additional information to be added to a disk log file, based on the fault category, when the notification of a fault is received._	MCI	A	TC029.001	Demo
C-MSS-60080	The MSS Fault Management Application Service shall have the capability to establish, view, modify and delete thresholds on performance metrics it measures._	MCI	A	TC029.001	Demo
C-MSS-60100	The MSS Fault Management Application Service shall have the capability to poll for the detection of fault/performance information._	MCI	A	TC029.002	Demo
C-MSS-60110	The MSS Fault Management Application Service shall be capable of receiving fault notifications.	MCI	A	TC029.002	Demo
C-MSS-60120	The MSS Fault Management Application Service shall have the capability to define the frequency with which polling is done for the detection of fault/performance information._	MCI	A	TC029.002	Demo

C-MSS-60130	The MSS Fault Management Application Service shall provide the capability to detect the following types of faults, and errors and events: _a._communications software version mismatch errors _b._communication software configuration errors _c._the following errors in communication hardware: __1. host not reachable __2. router not reachable __3. errors and failures of communication links _d._Errors in the communications protocols supported _e._degradation of performance due to established thresholds being exceeded _f._Peripherals _g._Databases _h._Applications: __1. process missing (Application or COTS product) __2. process in a loop	MCI	A	TC029.002	Demo
C-MSS-60140	The MSS Site Fault Management Application Service shall have the capability to generate a fault notification when a predefined threshold on a performance metric is exceeded.	MCI	A	TC029.001	Demo
C-MSS-60150	The MSS Fault Management Application Service shall provide the capability to receive fault notifications from: _a._SNMP agents _b._Applications	MCI	A	TC029.002	Demo
C-MSS-60160	The MSS EMC Fault Management Application Service shall have the capability to receive notifications of detected faults and degradation of performance from: a._Site fault management applications b._Other external systems as defined in Section 5.1.	MCI	A	TC029.002	Demo

C-MSS-60170	The MSS EMC Fault Management Application Service shall be capable of requesting fault notifications and performance degradation data from : _a._Site Fault Management Applications _b._Other external systems as defined in Section 5.1.	EMCI	A	TC029.002	Demo
C-MSS-60180	The MSS EMC Fault Management Application Service shall be capable of receiving summarized fault notification and performance degradation data from: a._Site fault management applications b._Other external systems as defined in Section 5.1.	MCI	A	TC029.002	Demo
C-MSS-60190	The MSS Fault Management Application Service shall use the Logging Services to record each detected fault.	MCI	A	TC029.002	Demo
C-MSS-60200	The MSS Fault Management Application Service shall have the capability to generate the following types of notifications for detected faults : _a._a change in the color of an icon on a display _b._a message in a pop-up notification window _c._logging the following fault information to a disk log file: __1. fault type __2. date and time of occurrence of the fault __3. IP address of the source of the notification __4. fault data received with the notification __5. operator-defined descriptive text _d._audible alert	MCI	A	TC029.002	Demo
C-MSS-60210	The MSS Fault Management Application Service shall maintain a list of external service providers, M&O operators, and applications to be notified in the event that a specified fault is detected.	MCI	A	TC029.002	Demo

C-MSS-60220	The MSS Fault Management Application Service shall have the capability to send the notification of a fault to registered recipients._	MCI	A	TC029.002	Demo
C-MSS-60230	The MSS Fault Management Application Service shall have the capability of generating a notification within a maximum of five minutes of fault detection.	MCI	A	TC029.002	Demo
C-MSS-60300	The MSS Fault Management Application Service shall provide the capability to identify routes between selected pairs of hosts on the ESN.	MCI	A	TC029.003	Demo
C-MSS-60310	The MSS Fault Management Application Service shall provide utilities to perform diagnostics and testing of the following for the purpose of fault isolation: _a._connectivity between pairs of ECS hosts and ECS routers _b._ability to reach hosts and routers _c._availability of network services at hosts_	MCI	A	TC029.003	Demo
C-MSS-60320	The MSS Fault Management Application Service shall provide, for selective use as a debugging aid, the capability to perform packet tracing of protocols used in ECS._	MCI	A	TC029.003	Demo
C-MSS-60330	The MSS Fault Management Application Service at each site shall have the capability to perform periodic testing of all ECS communication links at that site to verify that they are operational._	MCI	A	TC029.003	Demo
C-MSS-60340	The MSS Fault Management Application Service shall be capable of verifying the operational status of a host.	MCI	A	TC029.003	Demo
C-MSS-60350	The MSS Fault Management Application Service shall have the capability to periodically execute diagnostic tests in order to isolate, characterize and identify a fault._	MCI	A	TC029.003	Demo

C-MSS-60360	The MSS Fault Management Application Service shall provide the capability to execute vendor diagnostics in order to diagnose faults traced to hardware equipment.	MCI	A	TC029.003 (test case needs clarification)	Demo
C-MSS-60370	The MSS Fault Management Application Service at the SMC shall be capable of sending gathered isolation, location, identification and characterization of reported faults data to the level of subsystem and equipment to the following: _a._the site Fault Management Applications _b._other external systems as defined in Section 5.1.	MCI	A	TC029.0030	Demo
C-MSS-60380	The MSS Fault Management Application Service at the sites shall isolate, locate, and identify faults, identify subsystem, equipment and software faults, and identify the nature of the faults detected within its site._	MCI	A	TC029.003	Demo
C-MSS-60390	The MSS Fault Management Application Service at the sites shall, for faults detected within its site, isolate, locate, and identify faults to the level of: _a._subsystem _b._equipment _c._software	MCI	A	TC029.003	Demo
C-MSS-60395	The MSS Fault Management Application Service shall be capable of retrieving records of detected faults.	MCI	A	TC029.004	Demo
C-MSS-60400	The MSS EMC Fault Management Application Service shall support, maintain, and update system fault management policies and procedures, to include: a. Fault Identification, b. Fault priorities, c. Recovery or corrective actions.	MCI	A	TC029.004	Demo
C-MSS-60410	The MSS Site Fault Management Application Service shall have the capability to receive Fault Management Policies and Procedures from the EMC._	MCI	A	TC029.004	Demo

C-MSS-60420	The MSS Fault Management Application Service shall interface with the MSS Configuration Management Application Service and schedule a change in the configuration of the site when such a change in the configuration of the site is deemed necessary to recover from a fault._	MCI	A	TC029.004	Demo
C-MSS-60500	The MSS EMC Fault Management Application Service shall coordinate the recovery from conditions of performance degradation and faults with the sites and external network service providers.	MCI	A	TC029.002	Demo
C-MSS-60510	The MSS Fault Management Application Service at the EMC shall coordinate, as necessary via directives and instructions, the recovery from faults reported from a site.	MCI	A	TC029.005	Demo
C-MSS-60520	The MSS Fault Management Application Service shall provide the capability to allow the specification and execution of action routines in response to the notification of a fault.	MCI	A	TC029.005	Demo
C-MSS-60530	The MSS Fault Management Application Service shall provide the capability to pass parameters to action routines.	MCI	A	TC029.005	Demo
C-MSS-60540	The MSS Fault Management Application Service shall utilize office automation support tools for the generation of directives and instructions for recovery from faults within its site.	MCI	A	TC029.005	Demo
C-MSS-60600	The MSS Fault Management Application Service shall have the capability to generate, on an interactive and on a scheduled basis, reports on performance/error data that it has been configured to collect.	MCI	A	TC029.006	Demo

C-MSS-60610	The MSS Fault Management Application Service shall have the capability to build histories for different types of errors and events detected, for the purpose of analysis.	MCI	A	TC029.006	Demo
C-MSS-60620	The MSS Fault Management Application Service shall have the capability to redirect reports to: a. console, b. disk file, c. printer	MCI	A	TC029.006	Demo
C-MSS-66000	The MSS performance management application service shall be capable of monitoring the performance of the following ECS components a._network components _1. routers _2. links _3. bridges _4. gateways b._hosts c._operating systems d._peripherals e._databases	MCI	A	TC028.006	Demo
C-MSS-66010	The MSS performance management application service shall be capable of monitoring ECS component protocol stack performance parameters defined in IETF RFC 1213.	MCI	A	TC028.006	Demo
C-MSS-66020	The MSS Performance Management Application Service shall be capable of monitoring ethernet-like device performance parameters as specified in IETF RFC 1623.	MCI	A	TC028.006	Demo
C-MSS-66030	The MSS performance management application service shall be capable of receiving managed object definitions for each managed object.	MCI	A	TC028.006	Demo
C-MSS-66040	The MSS performance management application service shall be capable of specifying which available performance metrics are to be gathered from each individual managed object.	MCI	A	TC028.006	Demo

C-MSS-66050	The MSS performance management application service shall be capable of requesting performance data from each individual managed object: a._at configurable intervals b._on demand.	MCI	A,	TC028.006	Inspection Demo
C-MSS-66060	The MSS performance management application service shall be capable of receiving requested performance data from ECS components.	MCI	A	TC028.001	Demo
C-MSS-66070	The MSS Performance Management Application Service shall be capable of receiving unrequested performance data from ECS components.	MCI	A	TC028.001	Demo
C-MSS-66080	The MSS performance management application service shall be capable of retrieving the following data for all network component interfaces: a._operational status b._type c._speed d._octets in/out e._packets in/out f._discards in/out g._errors in/out	MCI	A	TC028.002	Demo
C-MSS-66090	The MSS Performance Management Application Service shall have the capability to collect the following performance information about communication protocol stacks on managed devices: _a._number of transport layer messages received with errors _b._number of transport layer messages requiring retransmission _c._number of transport layer messages received that could not be delivered _d._number of jetwork layer messages received with errors _e._number of network layer messages received that could not be delivered _f._number of network layer messages that were discarded_	MCI	A	TC028.003	Demo

C-MSS-66100	The MSS performance management application service shall be capable of retrieving the following data for all hosts: a._total CPU utilization b._memory utilization c._physical disk i/o's d._disk storage size e._disk storage used f._number of active processes g._length of run queue h._network i/o's (packets) i._network errors	MCI	A	TC028.002	Demo
C-MSS-66120	The MSS performance management application service shall be capable of determining the operational state of all network components, hosts, and peripherals to be: a._on-line b._off-line c._in test mode	MCI	A	TC028.001	Demo
C-MSS-66130	The MSS performance management application service shall be capable of receiving operational state change notifications from network components, hosts, applications, and peripherals.	MCI	A	TC028.005	Test
C-MSS-66135	The MSS Performance Management Application Service shall have the capability to calculate the following statistics for the purpose fo supporting RMA analysis for managed objects: a. Mean Down Time (MDT) b. Mean Time Between Maintenance (MTBM) 1. Mean Time Between Preventive Maintenance (MTBPM) 2. Mean Time Between Corrective Maintenance (MTBCM) c. Mean Time To Repair (MTTR)	MCI	A	TC028.008	Analysis

C-MSS-66137	The MSS Performance Management Application Service shall retain the calculated RMA statistics in a repository accessible for further analysis by the M&O staff.	MCI	A	TC028.008	Analysis
C-MSS-66140	The MSS EMC Performance Management Application Service shall have the capability to request performance data from: a._Site performance management applications b._Other external systems as defined in Section 5.1.	MCI	A	TC028.005	Test
C-MSS-66150	The MSS EMC Performance Management Application Service shall be capable of receiving performance data from: a._Site performance management applications b._Other external systems as defined in Section 5.1.	MCI	A	TC028.005	Test
C-MSS-66160	The EMC Performance Management Application Service shall be capable of receiving summarized performance data from: a._Site performance management applications b._Other external systems as defined in Section 5.1.	MCI	A	TC028.005	Demo
C-MSS-66170	The MSS performance management application service shall log ECS performance data in the History Log using APIs provided by CSS.	MCI	A	TC028.005	Demo

C-MSS-66180	The MSS performance management application service shall provide scripts to generate the following types of network statistics for a configurable period of time for performance data stored in the Management Database: a._average b._median c._maximum d._minimum e._ratios f._rates g._standard deviations.	MCI	A	TC028.005	Demo
C-MSS-66190	The MSS performance management application service shall provide a configurable number of thresholds for each performance metric.	MCI	A	TC028.004	Demo
C-MSS-66200	The MSS EMC performance management application service shall be capable of creating a list of suggested initial threshold values for each performance metric.	MCI	A	TC028.004	Demo
C-MSS-66210	The MSS EMC performance management application service shall be capable of sending a list of suggested initial thresholds for each performance metric to the MSS site performance management application service via CSS services.	MCI	A	TC028.004	Demo
C-MSS-66220	The MSS site performance management application service shall be capable of receiving a list of suggested initial thresholds for each performance metric from the MSS EMC performance management application service.	MCI	A	TC028.004	Demo
C-MSS-66230	The MSS performance management application service shall allow each performance metric threshold to be configurable.	MCI	A	TC028.004	Test

C-MSS-66240	The MSS performance management application service shall be capable of evaluating each performance metric against defined thresholds.	MCI	A	TC028.004	Demo Test
C-MSS-66250	The MSS performance management application service shall record an event in the local History Log whenever a threshold is crossed.	MCI	A	TC028.005	Test
C-MSS-66260	The MSS performance management application service shall provide queries that generate performance statistics from performance data stored in the Management Database.	MCI	A	TC028.005	Test Demo
C-MSS-66270	The MSS performance management application service shall store generated performance statistics.	MCI	A	TC028.005	Demo
C-MSS-66280	The MSS site performance management application service shall be capable of extracting summarized site status information from logged performance data.	MCI	A	TC028.005	Demo Test
C-MSS-66290	The MSS site performance management application service shall be capable of sending summarized status information for that site to the MSS EMC performance management application service.	MCI	A	TC028.005	Test
C-MSS-66300	The MSS EMC performance management application service shall log received summarized site status.	MCI	A	TC028.005	Demo

C-MSS-66310	The MSS performance management application service shall be capable of retrieving the following science algorithm performance data from local History Logs using CSS-provided APIs: a._algorithm name b._algorithm version c._start time d._stop time e._CPU utilization f._memory utilization g._disk reads h._disk writes	MCI	A	TC028.005	Demo Test
C-MSS-67000	The MSS EMC performance management application service shall be capable of extracting values of performance metrics gathered for a specified managed network component over a configurable period of time from the Management Database.	MCI	A	TC028.004	Test Demo
C-MSS-67010	The MSS EMC performance management application service shall be capable of generating a graph of the extracted performance metric values.	MCI	A	TC028.006	Demo
C-MSS-68000	The MSS performance management application service shall be capable of graphically displaying the operational state of managed objects through the MUI service.	MCI	A	TC028.006	Demo
C-MSS-68010	The MSS performance management application service shall be capable of displaying M&O staff-selected performance statistics through the MUI in tabular and graphical formats.	MCI	A	TC028.008	Demo
C-MSS-68020	The MSS performance management application service shall be capable of printing M&O staff-selected performance statistics.	MCI	A	TC028.008	Demo

C-MSS-68030	The MSS performance management application service shall be capable of receiving system resource utilization information requests from the SDPS Data Processing subsystem.	MCI	A	TC028.008	Demo
C-MSS-68040	The MSS performance management application service shall be capable of providing the following current system resource utilization information to the SDPS Data Processing subsystem: a._CPU utilization b._memory utilization c._disk i/o's (per second)	MCI	A	TC028.008	Demo Test
C-MSS-68050	The MSS performance management application service shall be capable of receiving resource utilization information requests from the SDPS Data Server subsystem.	MCI	A	TC028.008	Demo
C-MSS-68060	The MSS performance management application service shall be capable of providing the following current resource utilization information to the SDPS Data Server subsystem:.	MCI	A	TC028.008	Test
C-MSS-68070	The MSS performance management application service shall be capable of receiving resource utilization information requests from the SDPS Client subsystem.	MCI	A	TC028.008	Test
C-MSS-68080	The MSS performance management application service shall be capable of providing the following current resource utilization information to the SDPS Client subsystem.	MCI	A	TC028.008	Test
C-MSS-68090	The MSS Performance Management Application Service shall have the capability to generate reports from collected management data	MCI	A	TC028.008	Test

C-MSS-68100	The MSS Performance Management Application Service shall have the capability to redirect reports to: a. console, b. disk file, c. printer	MCI	A	TC028.008	Test
C-MSS-69000	The MSS performance management application service shall maintain operational benchmark test procedures.	MCI	A	TC028.007	Test
C-MSS-69010	The MSS site performance management application service shall receive and maintain operational benchmark test results.	MCI	A	TC028.007	Demo
C-MSS-69020	The MSS performance management application service shall be capable of performing operational benchmark tests.	MCI	A	TC028.007	Demo
C-MSS-69030	The MSS performance management application service shall be capable of providing results of benchmark tests and results of predefined tests to the local M&O staff for validation.	MCI	A	TC028.007	Demo
C-MSS-70100	The MSS site Security Management Application Service shall provide the capability to set, maintain, and update access control information for ECS resources._	MCI	A	TC024.006	Demo
C-MSS-70110	The MSS site Security Management Application Service shall provide the capability to specify privileges for authorized users and user groups for access to ECS resources._	MCI	A	TC024.002	Demo
C-MSS-70120	The MSS site Security Management Application service shall provide the mechanism, for each ECS host, to allow or deny incoming requests from specific hosts to services._	MCI	A	TC025.002	Demo

C-MSS-70130	The MSS site Security Management Application Service shall provide a command line interface and a GUI for the management of the following security databases: a._Authentication Database b. _Authorization Database c._Network Database	MCI	A	TC024.006	Demo
C-MSS-70300	The MSS site Security Management Application Service shall have the capability to perform the following types of security tests: a._password auditing b._file system integrity checking c._auditing of user privileges d._auditing of resource access control information	MCI	A	TC024.006	Demo
C-MSS-70310	The MSS site Security Management Application Service shall have the capability to perform security testing on a periodic and on an interactive basis.	MCI	A	TC024.006	Demo
C-MSS-70320	The MSS site Security Management Application Service shall have the capability to send the results of the tests to the EMC Security Management Application Service.	MCI	A	TC024.006	Demo
C-MSS-70330	The MSS EMC Security Management Application Service shall have the capability to request, support, manage and maintain security testing for sites.	MCI	A	TC024.014	Test
C-MSS-70340	The MSS EMC Security Management Application Service shall have the capability to request security testing of the sites on a scheduled and an interactive basis	MCI	A	TC024.014	Test Demo
C-MSS-70350	The MSS EMC Security Management Application Service shall have the capability to receive the results of security tests performed at the sites.	MCI	A	TC024.014	Test Demo

C-MSS-70400	The MSS EMC Security Management Application Service shall have the capability to receive notifications of security events from the site Security Management Application Services._	MCI	A	TC024.014	Test Demo
C-MSS-70410	The MSS EMC Security Management Application Service shall have the capability to receive security audit trails from the site Security Management Application Services._	MCI	A	TC024.014	Demo
C-MSS-70420	The MSS EMC Security Management Application Service shall have the capability to analyze security audit trails for the purpose of detecting intrusions._	MCI	A	TC024.014	Demo
C-MSS-70430	The MSS site Security Management Application Service shall provide the capability to designate a user or a group of users to receive a notification upon the detection of an intrusion._	MCI	A	TC024.006	Analysis Demo
C-MSS-70440	The MSS site Security Management Application Service shall provide the capability to notify designated M&O staff upon the detection of an intrusion._	MCI	A	TC024.006	Demo
C-MSS-70450	The MSS site Security Management Application Service shall have the capability to periodically analyze the security audit trails to detect the following types of intrusions: a._Login failures b._Unauthorized access to ECS resources c._Break-ins_	MCI	A	TC024.006	Demo
C-MSS-70460	The MSS site Security Management Application Service shall have the capability of generating a notification within a maximum of five minutes of the detection of an intrusion.	MCI	A	TC024.006	Demo

C-MSS-70500	The MSS EMC Security Management Application Service shall have the capability to coordinate with the site Security Management Application Services, via directives and instructions, the recovery from security compromises._	MCI	A	TC024.014	Demo
C-MSS-70510	The MSS site Security Management Application Service shall, upon the detection of a compromise, isolate the compromised input I/O, and the compromised area's output I/O until the compromise has been eliminated._	MCI	A	TC024.006	Demo
C-MSS-70520	The MSS EMC Security Management Application Service shall provide office automation support tools to enable the generation of directives and instructions for recovery from detected security events._	MCI	A	BC031.010	Demo
C-MSS-70530	The MSS EMC Security Management Application Service shall coordinate, as necessary via directives and instructions, the recovery from security events reported from a site. _	MCI	A	TC024.014	Demo
C-MSS-70700	The MSS Security Management Application Service shall have the capability to generate reports on the following: a._Login failures b._Unauthorized access to ECS resources c._Break-ins_	MCI	A	TC024.011	Demo
C-MSS-70710	The MSS Security Management Application Service shall have the capability to generate reports from collected management data.	MCI	A	TC024.011	Demo
C-MSS-70720	The MSS Security Management Application Service shall have the capability to redirect reports to: a. console, b. disk file.	MCI	A	TC024.011	Demo

C-MSS-75000	The MSS accountability management service shall provide the capability to maintain a user profile database that stores the following information for each registered user: a. Name b. User ID c. Password d. Assigned privileges e. Mailing address f. Telephone number g. Product shipping address h. E-mail address i. Organization (optional) j. Project affiliation(s) (optional) _1. project name _2. project principal investigator k. User group	EMCI	A	TC030.003 TC030.005 TC030.006	Test Demo
C-MSS-75010	The MSS accountability management service shall be capable of receiving user profile records entered by M&O personnel.	MCI	A	TC030.004	Demo
C-MSS-75020	The MSS Accountability Management Service shall create a new user account whenever a new record is added to the user profile database.	MCI	A	TC030.005	Test
C-MSS-76000	The MSS accountability management service shall be capable of retrieving user activity data (user id, type of user activity, data items used (browsed, searched, or ordered), and date/time of activity) from History Logs created by the SDPS Data Server, Data Processing, and Client subsystems.	MCI	A	TC030.005	Test
C-MSS-76010	The MSS accountability management service shall be capable of querying, via the Management Data Access service, user activity data stored in the Management Database.	MCI	A	TC030.006	Test

C-MSS-76020	The MSS accountability management service shall be capable of retrieving activities associated with a particular user or data item via the Management Data Access service.	MCI	A	TC030.005	Test
C-MSS-76030	The MSS site Security Management Application Service shall provide the mechanism to log, for each ECS host, incoming access attempts via: a. telnet b. FTP c. rlogin d. finger.	MCI	A	TC030.005	Test
C-MSS-76040	The MSS Accountability Management Service shall be capable of reporting audit information to M&O staff via the MUI service.	MCI	A	TC030.006	Test
C-MSS-77000	The MSS accountability management service shall be capable of retrieving data processing information (instrument used and date/time of ingest or algorithm used (name and version) and date/time or processing) from records generated by the SDPS Data Processing subystem.	MCI	A	TC030.006	Demo
C-MSS-77010	The MSS accountability management service shall be capable of querying via the Management Data Access service all data processing information stored in the Management database.	MCI	A	TC030.006	Test
C-MSS-77030	The MSS accountability management service shall be capable of retrieving all data processing information logged for a specified data item.	MCI	A	TC030.006	Test
C-MSS-77040	The MSS accountability management service shall be capable of accepting queries for the status of a particular ordered data item from the SDPS Client subsystem.	MCI	A	TC030.006	Test

C-MSS-77050	The MSS accountability management service shall be capable of interfacing with the SDPS subsystems to determine the status of an ordered data item to be: a. Item in queue for processing b. Item currently being processed c. Item successfully processed d. Error in processing e. Error in request	MCI	A	TC030.006	Test
C-MSS-77060	The MSS accountability management service shall be capable of reporting the requested status of an ordered data item to the SDPS Client subsystem.	MCI	A	TC030.006	Test Demo
C-MSS-77070	The MSS accountability management service shall be capable of searching local history logs to find processing data for an ordered data item.	MCI	A	TC030.006	Test
C-MSS-77080	The MSS Accountability Management Service shall have the capability to generate reports from collected management data.	MCI	A	TC030.006	Test
C-MSS-77090	The MSS Accountability Management Service shall have the capability to redirect reports to: a. console, b. disk file and c. printer.	MCI	A	TC030.006	Test
C-MSS-90020	The DBMS shall support a client-server design paradigm.	MCI	A	BC031.008	Test
C-MSS-90030	The DBMS shall provide security access control based upon userid, role and privileges for the following: a. database, b. database object, c. database operations.	MCI	A	BC031.008	Test
C-MSS-90060	The DBMS shall provide an SQL interface with query, update, and administrative functions capabilities.	MCI	A	BC031.008	Inspection
C-MSS-90070	The DBMS shall be in compliance with the SQL-2 of Federal Information Processing System Publication (FIPS PUB) 127-1.	MCI	A	BC031.008	Demo

C-MSS-90080	The DBMS shall provide the capability to generate ad hoc statistics from management data	MCI	A	BC031.008	Inspection
C-MSS-90120	The DBMS shall be compatible with the ECS management framework to support the import of the ECS management framework data.	MCI	A	BC031.008	Inspection
C-MSS-90140	The DBMS shall support, or be accessed via, CSS session-establishment services.	MCI	A	BC031.008	Demo
C-MSS-90150	The DBMS shall support access structures (i.e., single-level indexes, multilevel indexes) to improve the efficiency of retrieval of management data.	MCI	A	BC031.008	Demo
C-MSS-90160	The DBMS shall support the X/Open environment features to include the following: a. Hardware independence b. Operating systems independence c. Network protocols independence	MCI	A	BC031.008	Test Demo
C-MSS-90170	The DBMS shall provide the following bulk data load capabilities: a. direct writes from data files to database b. loading of files containing fixed and variable length records c. incremental bulk load d. Maintain indexes during data loads	MCI	A	BC031.008	Test Demo
C-MSS-90180	The DBMS shall provide the following database backup capabilities: _a. Entire database _b. Incremental data _c. User specified database items.	MCI	A	BC031.008	Demo
C-MSS-90190	The DBMS shall provide capabilities for specifying frequency, time, and type of backups.	MCI	A	BC031.008	Demo

C-MSS-90200	The DBMS shall perform on-line disk management functions to include: a. Relocation of database files to different disks b. Expansion of database size by adding new physical data files to it on-line c. Dynamic pre-allocation of contiguous space for tables d. Database objects and indexes can span physical files e. Database objects and indexes can exist on different disks	MCI	A	BC031.008	Demo
C-MSS-90210	The DBMS shall support the following features: a. Data compression of nulls and variable length character strings, and indexes b. Space reclaimed from deleted records automatically c. Variable-length column storage	MCI	A	BC031.008	Demo
C-MSS-90230	The DBMS shall provide a transaction roll backward capability to a specified time or state: a. Restore a database b. Restore all or operator selected database objects of any database	MCI	A	BC031.008	Demo
C-MSS-90240	The DBMS shall provide for automatic database recovery including: a. A means to automatically restore undamaged portions of a database and recover work in progress after a system or component failure b. A means to achieve dynamic backout of database modifications, performed by a failing transaction, that does not affect separate, concurrent tasks	MCI	A	BC031.008	Test
C-MSS-90260	The DBMS shall provide a capability to export, archival, and restore a database.	MCI	A	BC031.008	Demo
C-MSS-90280	The DBMS shall provide the capability to issue and record a database checkpoint.	MCI	A	BC031.008	Demo

C-MSS-90290	The DBMS shall provide an audit trail of chronological activities in the database.	MCI	A	BC031.008	Test Demo
C-MSS-90500	The Report Generator shall be compatible with the DBMS	MCI	A	BC031.011	Demo
C-MSS-90510	The Report Generator shall provide a Motif base Graphical User Interface (GUI) for creating ad hoc reports.	MCI	A	BC031.011	Demo
C-MSS-90520	The Report Generator shall have the capability to generate ad hoc reports from management data maintained in the DBMS	MCI	A	BC031.011	Demo
C-MSS-90530	The Report Generator shall provide the capability to format reports to include the report: a. title, b. header, c. footer, d. page number, e. date/time of report.	MCI	A	BC031.011	Demo
C-MSS-90570	The Report Generator shall have the capability to generate charts and graphs (e.g., bar, pie, line, etc.) from management data maintained in the DBMS.	MCI	A	BC031.011	Demo
C-MSS-90600	The Report Generator shall provide the capability to redirect generated reports to: a. console, b. disk file, c. printer	MCI	A	BC031.011	Demo
C-MSS-91010	The MSS Office Automation word processing capability shall facilitate the: a._preparation, revision, and recording of documents, messages, reports, and data b._import, transformation, and editing of documents produced by other word processing packages c._insertion of worksheet and graphic images into documents, messages, and reports d._transfer of document, message, and report information to spreadsheet and graphics applications e._printing of documents, messages, reports, and data	MCI	A	BC031.010	Demo

C-MSS-91020	The MSS Office Automation shall provide a spreadsheet capability that: a._simulates and displays an accountant's worksheet b._enables revisions and calculations on the displayed worksheet's data c._enables transfer of the worksheet data to word processing and graphics applications d._enables printing of worksheet information.	MCI	A	BC031.010	Demo
C-MSS-91030	The MSS Office Automation shall provide a graphics capability that enables: a._the development, modification, recording, and printing of graphic images b._the transfer of graphics images to word processing documents, messages, and reports.	MCI	A	BC031.010	Demo

Appendix C. Build/Thread to Test Case Description Matrix

Build/ Thread	Thread/ Test Case ID	Sub	Service class	Source	SLOC	Trk	EP
Internetwork/ Internetworking	TC017	ISS	Transport (T)	COTS	n/a	F	n/a
Internetwork/ Internetworking	TC017	ISS	Network (N)	COTS	n/a	F	n/a
Internetwork/ Internetworking	TC017	ISS	Data Link/ Physical (D)	COTS	n/a	F	n/a
Comm Services	TC018 BC023	CSS	Object Passing	Dev. + COTS	1,500	I	EP6
Comm Services	TC018 BC023	CSS	Message Passing	Dev. + COTS	8,000	I	EP6
Comm Services	TC018 TC022 BC023	CSS	Lifecycle Service	Dev. + COTS	4,000	I	EP6
Comm Services/ Directory Naming Service	TC019	CSS	Directory/Naming Service	Dev.	5,500	I	EP6
Comm Services/ Distributed File Service	TC020	CSS	File Access Service	Dev. + COTS	6,500	I	EP6
Comm Svcs/Email/ BB Svc	TC021	CSS	Bulletin Board (BB)	Glue + COTS	1,000	I	EP6
Comm. Services /Email/ BB Services	TC021	CSS	Electronic Mail Service w/ MIME	Dev.	500	I	EP6
System Security/ Security Management/ Accountability	TC024	CSS	Security Service	Dev. + COTS	7,500	I	EP6
System Security/ Security Management	TC024	MSS	Security Mgt: Compliance Mgt	Dev	1,500	F	n/a

Build/ Thread	Thread/ Test Case ID	Sub	Service class	Source	SLOC	Trk	EP
System Security/ Security Management	TC024	MSS	Security Mgt: Reporting	Dev	0	F	n/a
System Security/ Security Management	TC025	MSS	Security Mgt: Intrusion Detection	Dev + COTS	1,500	F	n/a
System Security/ Accountability	BC026	MSS	Security Mgt: Audit Info Collection	Dev	0	F	n/a
Mgmt. Svcs/ Sys Logistic Mgmt	TC027	MSS	Configuration Management	Dev + COTS	1,500	F	n/a
Comm. Services/ Performance Mgmt.	TC028	CSS	Event Logger Service	Dev	3,000	I	EP6
Comm. Services/ Performance Mgmt.	TC028	CSS	Event Service	Dev. + COTS	6,000	I	EP6
Management Services/ Performance Mgmt.	TC028	MSS	Performance Mgt: Monitoring	Dev.	500	F	n/a
Management Services/ Performance Mgmt.	TC028	MSS	Performance Mgt: Reporting	COTS	500	F	n/a
Management Services/ Performance Management	TC028	MSS	Performance Mgt: Analysis	COTS	2000	F	n/a
Management Services/ Fault Management	TC029	MSS	Fault Mgt: Fault Recovery	Glue	500	F	n/a
Management Services/ Fault Management	TC029	MSS	Fault Mgt: Reporting	Glue	500	F	n/a

Build/ Thread	Thread/ Test Case ID	Sub	Service class	Source	SLOC	Trk	EP
Management Services/ Accountability	TC030	MSS	Accountability Mgt: Accountability	Dev. + COTS	1,000	F	n/a
Management Services/ Accountability	TC030	MSS	Accountability Mgt: User Registration	Dev. + COTS	2,000	F	n/a
Management Services/ Internetworking	BC031	MSS	Mgt Data Access	Dev.	4,000	F	n/a
Management Services/ Internetworking	BC031	MSS	Management Agents	Dev + COTS	3,500	F	n/a
Management Services/ Internetworking	BC031	MSS	Maps & Collections	Glue + COTS	500	F	n/a
Management Services/ Management Framework	BC031	MSS	Management Framework	COTS	1,000	F	n/a
Management Services	BC031	MSS	DBMS	COTS	2,000	F	n/a
Total Estimated SLOC Development for Release A				69.5k			

This page intentionally left blank.

Abbreviations and Acronyms

ACL	access control list
AI&T	Algorithm Integration and Test
API	application programming interface
ATM	asynchronous transfer mode
BBS	bulletin board server
CCB	configuration control board
CCR	configuration change request
CDR	Critical Design Review
CDRL	contract data requirements list
CDS	Cell Directory Service
CDSCP	cell directory service command program
CERES	Clouds and Earth's Radiant Energy System
CI	configuration item
CM	configuration management
CMAS	Configuration Management Application Service
CORBA	common object request broker architecture
COTS	commercial off-the-shelf
CRM	change request manager
CSC	computer software component
CSCI	computer software configuration item
CSMS	Communications and Systems Management Segment
CSR	Consent to Ship Review
CSS	Communications SubSystem
CSU	computer software unit
DAAC	Distributed Active Archive Center
DBMS	Data Base Management System
DCCI	Distributed Computing CI
DCE	Distributed Computing Environment
DCHCI	Distributed Computing Hardware CI

DCN	document change notice
DDTS	Distributed Defect Tracking System
DFD	data flow diagram
DFS	distributed file service
DID	data item description
DNS	Domain Name Service
DOF	distributed object framework
DTS	distributed time service
DV1	document version 1
Ecom	EOS Communications
ECS	EOSDIS Core System
EDC	EROS Data Center (DAAC)
EDF	ECS Development Facility
EDHS	ECS Data Handling System
EDOS	EOS Data and Operations System
EMC	enterprise management center
EOC	ECS Operations Center
EOS	Earth Observation System
EOSDIS	Earth Observation System Data Information System
EROS	Earth Resources Observation System
ESN	EOSDIS Science Network
ETR	Element Test Review
F&PRS	Functional and Performance Requirements Specifications
FDF	flight dynamics facility
FDDI	fiber distributed data interface
FMAS	fault management application service
FOS	Flight Operations Segment
FTP	file transfer protocol
GDS	Global Directory Service
GSFC	Goddard Space Flight Center
HiPPI	High Performance Parallel Interface

HWCI	Hardware CI
I&T	Integration and Test
IATO	Independent Acceptance Test Organization
ICD	Interface Control Document
IDL	interface definition language
IDR	internal design review
INCI	Internetworking CI
INHCI	Internetworking Hardware CI
IP	Internet protocol
IR-1	Interim Release one
ISO	International Standards Organization
ISS	Internetworking SubSystem
IST	Instrument Support Terminal
IV&V	Independent Verification and Validation
JPL	Jet Propulsion Laboratory
LAN	Local Area Network
LaRC	Langley Research Center
LIS	Lightning Imaging Sensor
LSM	local systems management
M&O	Maintenance and Operations
MACI	Management Agent Software CI
MCI	Management Software CI
MG1	Management one
MHCI	Management Hardware CI
MLCI	Management Logistics Software CI
MOC	Mission Operations Center
MRS	Malfunctions/failure Reports
MSFC	Marshall Space Flight Center
MSS	Management SubSystem
MUI	management user interface
NASCOM	NASA Communications

NISS	NASA Institutional Support System
NNTP	Network News Transfer Protocol
NOAA	National Oceanic and Atmospheric Administrator
NOLAN	Nascom Operational Local Area Network
NRCA	Noncomformance Reporting And Corrective Action
NSI	NASA Science Internet
OODCE	Object Oriented DCE
OMT	Object Modeling Technique
OSI	Open System Interconnect
OSPF	Open Shortest Path First (routing protocol)
OSI-RM	OSI - Reference Model
PDR	preliminary design review
PGS	Product Generation System
PI	Primary Investigator
PMAS	Performance Management Application Service
PSCN	Program Support Communications Network
RFC	request for comment
RFP	Request for Proposal
RIP	Router Information Protocol
RMA	Reliability, Maintainability, and Availability
RPC	remote procedure call
RRR	Release Readiness Review
RTM	requirements traceability matrix
SCF	Science Computing Facility
SDPF	Science Data Processing Facility
SDPS	Science Data Processing Segment
SEI	Software Engineering Institute
SMC	systems management center (ECS)
SMTP	Simple Mail Transport Protocol
SI&T	Systems Integration and Test
SLOC	Suggested Lines of Code

STD	state transition diagram
StP	Software Through Pictures
TBD	to be determined
TCP	Transmission Control Protocol
TMI	TRMM Microwave Image
TRMM	Tropical Rainfall Measuring Mission (joint US-Japan)
TRR	test readiness review
TSDIS	TRMM Science Data and Information System
UTC	universal time code
VIRS	Visisble Infrared Scanner
V0	Version Zero
VOB	Version Object Base